Небудь просто юзером. Продвинся, прочитав эту книгу.

Юзеры и Интернет

для "ЧАЙНИКОВ"™

Эта книга научит вас, как себя вести в интернете, что для чего предназначенно и что с этим делать.

Для сомневающихся



-=[MaPuK]=-

Содержание

Предисловие

Идея создания этой книги, заключается в том, что я на протяжении 3 лет запутался так, что выпутаться уже не смог. И все знания, которые я сумел вытащить из паутины, я познал не от людей, и не от уроков, а просто сидел на различных форумах, сайтах, читал информацию, смотрел видео уроки. И постепенно я начал понимать, что как работает, и зачем всё это нужно. Само собой, всё сразу не даётся, и та же история была и у меня. Сначала в 2003 году, впервые в жизни отправив обычную почту, я был настолько рад, что мне захотелось ещё и ещё. Позже заимев свой компьютер, я начал осваивать паутину, и день, за днём проводя в интернете всё своё свободное время, я понял – этой мой мир, и я в нём живу. Естественно отличие между реальным миром и миром в интернет просто огромное. В интернете я могу делать, что всё хочу, некто меня не за что не накажет, могу сказать всё что захочу и кому захочу, и т.д. Но вскоре мне надоело просто ходить с сайта на сайт, что сейчас и называется сёрфингом. О нём я опишу ниже. И я начал интересоваться более сложными вещами. По началу, как и все мы, начинающие пользователи сети, хотим или, что-то поломать, или что-то построить. Ну так как строить я ещё не научился, я пошел в поиск и стал искать статьи по взлому, Хаку, Вирусах, Троянах и прочих таких вещах, о которых я расскажу ниже. Добившись некоторых результатов, посмеявшись со своих друзей, я закончил свой походы по хакерским форумам. И начал пробовать, что-то строить. Набрав в том же поиске слова «Построить сайт», я наткнулся на огромное количество сайтов, где мне предлагали бесплатно делать сайт, только регистрируйся, заходи, и начинай настраивать свой сайт. Что я и сделал. Один, второй, третий сайт. Всё это жутко надоело, и я подумал: «Если люди сумели построить сайт, практически с нуля, то почему я не могу?». Получив в ответ от поисковой машины слово «Движок», что так же называется CMS (Content Management System). Мне показали форум, с огромным количеством пользователей и тем. Где я и остановился, каждый день я читал форум, читал и читал новые темы вопросы пользователей и ответы так называемых магистров сети, которые знали куда больше меня. Позже я начал спрашивать, получал ответы, получал слова вида: «Юзай поиск». Само собой многие термины я не знал, поэтому я, спрашивал и спрашивал. Вскоре по рассказам магистров, я начал практиковаться, на бесплатных хостингах, и постепенно пришел к отличным результатам. Через некоторое время магистры набравшись дозы знаний, как комар, который напился крови, они ушли с форума, а на их замену стали мы, новички которые стали своего рода магистрами. И я стал помогать новичкам, которые пришли на форум, куда позже меня. Вскоре форум закрыли, и все разбежались кто куда. У меня уже был Bape3 сайт, я вполные обороты, продвигал свой проект, разбирался во многих вещах, терминах, и в прочих web делах. На этом закончу предисловие, и скажу только о том, что все, что я узнал за это время, я хочу выложить в этой книге, а так же добавить информацию, более точную и правильную из сети интернет, дабы вам было более понятно, о чём конкретно идёт речь, и какие термины встречаются в интернете и как их понимать.

1. **Общий взгляд на web мир.**

История интернета.

Введение

Интернет – это разветвлённая глобальная сеть, посредством которой миллионы компьютеров обмениваются данными, используя определенные стандартные протоколы. Для подключения к сети Интернет достаточно простейшего модема. Купив модем (программы доступа к Интернет входят в состав операционной системы Windows) и, договорившись с фирмой-поставщиком услуг о правах доступа к Интернет, вы становитесь полноправным (с собственным адресом) членом глобального информационного сообщества и получаете возможность обмениваться сообщениями с другими абонентами сети, читать электронную прессу, участвовать в телеконференциях, совершать покупки и посещать выставки. Кроме того, ничто не помешает вам создать собственную Web-страницу…

История Интернета

В 60-е годы Министерство обороны США поставило задачу – разработать надёжную компьютерную сеть, которая должна была служить стратегическим интересам США. В основу концепции, надёжной сети была положена идея децентрализации. В распределенной децентрализованной системе частичный отказ в работе сети не приводил бы полной потере работоспособности.

В 1969 году большинство учреждений, связанных с министерством обороны, объединили собственные сети в так называемую сеть ARPAnet (Advanced Research Projects Agency Network). Университеты и другие учебные заведения проявили большой интерес к этой сети. Сеть ARPAnet можно считать прародителем современной сети Интернет.

Тем не менее, пришлось ждать 1993 года (когда число подключенных серверов перевалило за миллион), прежде чем сеть Internet приобрела очертания, близкие к сегодняшним, и провозгласила в качестве цели своего развития всеобщую информатизацию человечества. Многие частные предприятия и государственные учреждения были в восторге от возможностей глобальной системы связи, хотели пользоваться ее услугами и принимать участие в ее развитии. В то же время академические институты и учебные заведения форсировали дальнейшее развитие Internet.

1. **Общий взгляд на web мир**.

Основные сведения о WWW.

Когда мы говорим о HTML и Web-броузерах, речь идет только о части Internet: службе World Wide Web (сокращенно WWW или Web), - в последнее время вызвавшей бум среди пользователей.

Каждый подключённый к Интернету компьютерный сервер имеет собственный Интернет-адрес, который называется IP-адресом (Internet Protocol). Этот адрес состоит из четырёх разделенных точками чисел, каждое из которых имеет величину от 0 до 254.

Конечно же, эти числа нелегко запомнить, а поэтому каждому IP соответствует уникальное имя домена. Серверы имен хранят списки, определяющие соответствие между именами и номерами.

Если при обращении к Интернету IP-адрес задается не в числовой форме, выполняется автоматическое обращение к серверам имен с целью отыскать IP-эквивалента для заданного вами имени домена.

Программное обеспечение, необходимое для доступа к Интернету, предоставляет сервисный центр вашего поставщика Интернет-услуг.

1. **Общий взгляд на web мир.**

Обзор web браузеров.

Сейчас существует множество таких программ (браузеров) и перед пользователем стоит нелёгкий выбор. НюБоВ.НеТ рассмотрел лучшие из вариантов, возможные на сегодняшний день, и любезно предоставляет их вам. Все представленные программы являются бесплатными и обладают русскоязычным интерфейсом. Итак, начнём.

Internet Explorer 7



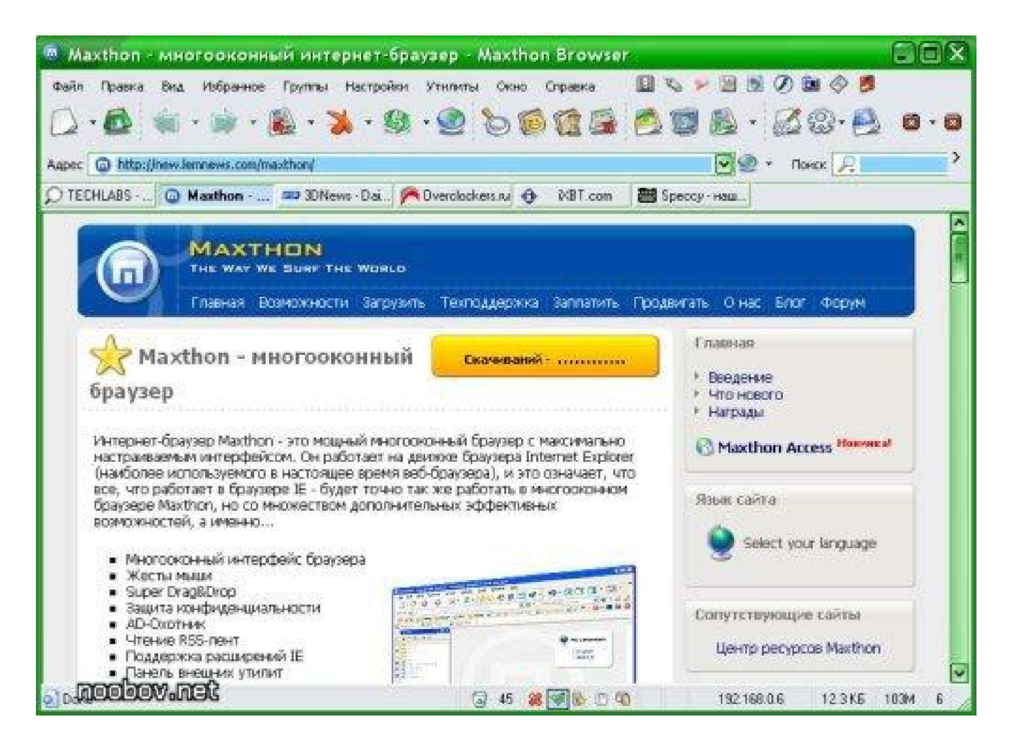
Internet Explorer является самым популярным мировым браузером. Но, к сожалению, такое большое количество пользователей использует его лишь по той причине, что просто не знают о существовании других более быстрых и удобных браузеров. Также существует необходимость, держать на компьютере сей продукт, потому что многие программы используют компоненты IE и без него корректно работать не будут. Ввиду популярности этого браузера многие сайты заточены именно под него. Что всё-таки иногда заставляет возвращаться к Internet Explorer.

Что появилось нового в седьмой версии браузера Internet Explorer? Наконец-то появилась нормальная система вкладок, которая позволила более-менее удобно работать в Интернете. Существенно повысилась скорость загрузки страниц, добавилась читалка новостей, фишинг-защита (защита от интернет-мошенничества). И ещё некоторые мелкие нововведения, которые, в общем-то, приближают уровень Internet Explorer к уровню других современных и популярных браузеров.

1. **Общий взгляд на** web **мир.**

IE7 поставляется в комплекте вместе с любой версией winows vista, а также бесплатно скачивается и устанавливается на winows xp. после проверки подлинности.

Maxthon 2.02.29



Этот браузер построен на основе ядра Internet Explorer. Фактически это тот же самый IE, но со значительно расширенной функциональностью. Например, в браузере реализована функция закрытия надоедающих всплывающих окон, а также очень удобное управление мышью. В программу встроена поддержка скинов, что не может не порадовать эстетов. В программе есть множество возможностей: быстрый перевод веб-страниц, автопрокрутка и многое другое.

1. **Общий взгляд на web мир.**

MyIE2



Данная программа является надстройкой над Internet Explorer, значительно расширяющая его функциональность. Некоторые функции, добавляемые этим пакетом, являются уникальными и не представлены ни в каких других браузерах. К примеру, в программе существует раздельный поиск софта, драйверов, рефератов, скриптов сразу по всем поисковикам. Функциональная панель ресурсов даёт возможность использовать множество различных инструментов: отправлять ICQ сообщения, смотреть программу ТВ и многое другое. Ну и ряд других нововведений, таких, как блокировка рекламы, которые уже стали стандартом для качественного браузера.

Значительно увеличена по сравнению с IE скорость работы и загрузки страниц. При этом все преимущества простого IE никуда не делись и остаются с вами. Идеальный выбор для тех, кто не хочет расставаться с Internet Explorer, но хочет работать с современным браузером.

1. **Общий взгляд на web мир.**

Mozilla FireFox



FireFox можно дополнить какой угодно функцией при помощи различных примочек. Итак, вы нашли интересное дополнение, что же делать дальше? Если вы нашли его во всемирной сети – то вам достаточно будет всего лишь нажать на ссылку расширения. Браузер сам обнаружит и установит её. Если файл находится на вашем жестком диске - тогда зайдите в меню «Файл», выберите пункт «Открыть файл», в строчке «Тип файлов» укажите «Все файлы» и выберите то расширение, которое хотите сейчас установить.

Для удаления откройте меню «Инструменты», загрузите «Менеджер расширений» – выберите расширение, нажмите кнопку «Удалить» и перезагрузите браузер.

1. **Общий взгляд на web мир.**

Opera 9.xx



Здесь же я опишу наиболее значительные дополнения, внесённые в девятую часть браузера, а также самые популярные возможности, которые отсутствуют в продуктах конкурентов.

Первое, о чём стоит упомянуть – это необычное управление Оперой. Вы можете управлять браузером как при помощи голоса (для этого необходимо установить необходимые библиотеки, размером около 10 мегабайт), а также при помощи специализированных мышиных жестов. На них остановлюсь чуть подробней.

Управление жестами осуществляется на основе удержания правой кнопки мыши и совершения различных, ранее заданных движений. Например, вы удерживаете правую кнопку мыши и делаете движение влево. Этим самым вы перейдёте на предыдущую страницу. Удерживая клавишу-модификатор shift, и совершив такое же движение вы перейдёте на самую первую страницу. Таким образом, вы можете осуществить практически любое действие при помощи жестов, что крайне удобно. Посмотреть и настроить список жестов вы можете, пройдя по следующему пути: «Инструменты» - «Настройки» - «Горячие переходы» - «Настройка мыши» - «Править».

Что касается нововведений, реализованных в девятой версии браузера Opera, то их тоже великое множество. Реализована поддержка виджетов, таких мини-приложений, размещающихся на вашем рабочем столе. Например, большие аналоговые часы или информер погоды. Чаще всего эти приложения не относятся напрямую к работе браузера,

1. **Общий взгляд на web мир**.

но следует привыкать, что просто браузеры уже не конкурентные. Скачать их и установить довольно легко – выбираете вкладку «Виджеты» - «Добавить» – вас перебрасывает на сайт http://widgets.opera.com/, где вы выбираете и скачиваете понравившееся приложение. Установка затруднений у вас не вызовет. Управление установленными приложениями осуществляется там же, только во вкладке «Управление».

Очень удобным нововведением в браузере стало отображение страниц-миниатюр. Когда пользователь открывает такое большое количество вкладок, когда прочтение адреса становится уже невозможным, пользователь просто наводит мышью на интересующую закладку и видит её изображение в миниатюре. Таким образом, не нужно прощелкивать все страницы в поисках нужной, а просто пару раз навести мышкой. Такой шаг очень хорошо экономит время.

Также в браузере Opera реализован удобный блокировщик содержимого сайтов, существует возможность индивидуально настроить правила отображения каждого портала в отдельности. Например, на одном сайте всплывающие окна носят рекламный характер, поэтому их лучше заблокировать. Зато многие форумы используют систему обмена личными сообщениями именно при помощи таких всплывающих окон.

2. Web **Мастерство**

Движки сайтов и форумов, и принцип их работы.

Что же такое движок сайта? Я попробую объяснить это самым простым языком. Слово движок от слова двигатель. То есть это система которая как и автомобиль управляет вашим сайтом, с функциями где вы как водитель можете изменять траекторию автомобиля простым поворотом руля. Так и здесь, движок это готовый PHP код (и не только PHP), где ваш сайт как правило уже готов принимать комментарии в новостях, имеет систему опросов, в котором уже как правило встроена админка для более простого управления вашим контентом. То есть вам после установки на ваш хостинг, такого скрипта, нечего больше ненужно делать, кроме как настроить ваш сайт, так как вам нравиться, и просто управлять сайтом. С таким же успехом можно поставить и не только скрипт новостей, или гостевых книг. В интернете так же куча очень мощных и удобных движков для управления форумами. Как правило, для движков и форумов в интернете есть огромное количество шкурок, то есть тем для оформления дизайна вашего сайта или форума. Это придаст вашему форуму или сайту особый вид и будет отличать ваш сайт от остальных ресурсов в сети. Каждый движок имеет свой официальный сайт, что придаёт более удобное скачивание и поиск информации, касающийся именно этого движка. Ознакомившись хотя бы с одним из них, у вас не составит труда, установить другой движок. Как правило, все скрипты (движки), написанные на PHP, используют базу данных, на языке MySQL. Для чего нужна такая база данных? А для того, чтобы вся информация не хранилась в файлах PHP, на ФТП сервере, а сохранялась в базе для её более удобной администрации и редактировании определенной информации на вашем сайте. Каждый из движков по своему особенный, один создан для огромного количества поситетелей, и в свою очередь имеет большинство функций так как: Добавления фотографии, подписей, своего инфо на форумах. Другие же движки форумов более простые в дизайне чтобы такой форум было легче загружать пользователю, и это не тратило бы его трафик, а так же для более низкого уровня запроса в базу данных, ведь чем больше запросов в базу данных, тем чаще тормозит сайт или форум. Ниже я хочу привести примеры движков сайтов и форумов чтобы вы более ориентировались:

1. Это мой первый движок, который попался мне в руки, и именно его я освоил сильнее остальных. Его имя Spaiz-Nuke. Этот движок основан на известном PHP-Nuke, но более сокращён и более быстр от мощного PHP-Nuke, и не занимает 10 мегабайт на ФТП сервере, а его код был сокращён до 1 мегабайта. К этому движку было написано огромное количество дизайнов, модулей и прочих аддонов. Он создан в основном для новостей, но так же имеет модуль фото-галереи, статей, гостевой книги, систему голосования, и прочее. Не стоить забывать о безопасности движков. Некоторые из них более защищённые некоторые менее. Ведь каждый

2. Web **Мастерство**

движок подвергается атаке со стороны хакеров, тем самым проверяет свою устойчивость в сети Интернет.

3. Ещё один очень мощных движок имеет огромное количество дополнений и тем для оформления, используется в основном для новостей и для варез сайтов. Почти каждый, варез сайт, который вы встречаете в интернете, он построен на движке Data-Life Engine. Он так же написан на языке PHP , но имеет добавки ajax для более быстрой и удобной работы в этом движке. Есть одно НО, данный движок является платным, поэтому скачивая nulled версию, вы рискуете, и попадаете под статью РФ, о нарушении авторских прав.

4. RunCMS – один из моих любимых движков. Стоит на моём сайте для новичков. Очень его уважаю за правильное написание кода PHP. А так же за его функциональность и работоспособность во всех браузерах. Довольно таки мощный, по уровню возможностей, и админки движка.

Поведаю так же о лучших движках, на мой взгляд, и для форумов. Но хочу, чтобы вы знали, что форум раскрутить для большой аудитории куда сложнее, чем сайт, ведь вам нужны не просто пользователи, которые пришли, скачали и ушли, вам нужны активные пользователи, которые будут посещать ваш форум ежедневно, и вносить свой вклад в его развитие и процветание. Поэтому знайте, когда выбираете, форум для большой публики, или для определённого количества пользователей.

1. IPB – Invision Power Board. Я считаю его лучшим движком для создания огромного форума. Несмотря на то, что он неслабо грузит базу, он настолько функционален, что я до сих пор не разобрался во всех его настройках. К нему создано огромное количество тем оформления, и сайты фанатов движка, и сайты по созданию тем, модулей, хаков, подсказки по редактированию кода, и множество другое. Всем рекомендую этот движок. Его история развивалась постепенно, начиная с самого простого, и дошла до наших дней идеальная защищенная версия.
2. vBulletin – в народе называют её Булка. Тоже, на мой взгляд, мощнейший двигатель для форума. Так же огромное количество тем оформления, хаков и модулей. Поставив этот движок, вы не пожалеете, но как я читал в ранних версиях есть уязвимости. Поэтому скачивая этот движок, его в поиске на уязвимости вписав названия движка и его версию.
3. phpBB – хороший движок, меньше грузит базу, но менее функционален чем два перечисленных выше. Тоже есть куча тем оформления на официальном сайте.

2. Web Мастерство

Продвижение сайта. Search Engines Optimization (SEO).

Ну конечно же продвижение сайта одна из самых главных проблем в создании сайта. Ведь научившись устанавливать движки, уделив настройке и украшениям сайта целую неделю, вы сталкиваетесь с проблемой, что на ваш сайт не заходят люди. И тогда вы начинаете думать, как же привлечь пользователей, и непросто которые зашли и ушли, а которые вернуться на ваш сайт, и день за днём будут на нём сидеть.

1. Ваш сайт должен обновляться ежедневно, будь- то варез, статьи о науке, видео уроки, или прочее, ведь пользователь, прочитав всю информацию, захочет ещё, но её нет, и он уйдёт на другой сайт. Поэтому ваш сайт должен быть полон информации, и она желательно должна соответствовать тематике вашего сайта. Ведь пользователь не хочет знать о состояниях на бирже, он пришел к вам на сайт, чтобы почитать статьи о том, как рисовать в Фотошопе, или писать на PHP, или любая другая информация, и ненужно совмещать кашу с борщем.
2. Ваш форум или сайт живёт самостоятельно без вашего участия, где пользователи знакомятся, общаются на форуме или сидят в чате, ваше участие заключается лишь в поддержке сайта, форума или чата. То есть представим, что вы администратор популярного сайта знакомств. Вы заходите на сайт только чтобы проверить, что всё работает, или добавить новую функцию, отредактировать PHP код, или ещё для чего то. Вы не нужны пользователям, они вас не замечают. Они сидят на вашем сайте и общаются со знакомыми или заводят новые знакомства. Так же происходит и с форумом. Но с чатом уже иначе. Ведь в чате, как правило, могут зайти нарушители. То есть вы пишите правила чата, а всегда есть кто-то, кто нарушает правила, материться, кидает свой сайт в виде рекламы, оскорбляет посетителей чата. За всем этим нужно следить, и эта работа для модератора. Модератор почти, как обычный пользователь, но имеет больше прав. Он имеет право наказать пользователя, удалить его из чата, или заблокировать (забанить) пользователя по имени или по IP-адресу. Тогда пользователь некогда не может войти в этот чат. Все эти права зависят от функциональности чата, ведь их тоже огромное количество в просторах интернета. Поэтому выбирая чат, убедитесь, что функции модератора включены в состав функций чата.

И так продвижение может быть или:

1. Реклама
2. Рассылка
3. Друзья по тематике
4. Каталоги
5. Поисковики

2. Web **Мастерство**

И так первое это реклама. Реклама это отличный способ заявить о вашем сайте. Вы добавляете вашу ссылку с картинкой-баннером на сайт. И позже видите рекламу своего сайта на кучи остальных сайтов. И пользователи нажимают на вашу картинку и заходят на ваш сайт. Таких способов рекламы куча: продажи ссылок, скупка участка пикселей на сайте, баннеро-обмен, и многое другое. Но такой способ раскрутить сайт стоит денег, и обычно немалых.

Рассылка. Этот способ хоть эффективный, но небезопасный. Ведь рассылая спам почту с составом письма, где есть ссылка на ваш сайт, со словами «СУПЕР МЕГА сайт – www.site.ru Вы рискуете быть заблокированными поисковыми системами, такими как Яндекс, или Гугл. То есть такой метод может принести успехи, но нужно быть аккуратным. Есть варианты рассылки на ICQ, на форумы, на электронную почту. Есть кучи программ, где отправка на форумы и по ICQ, уже автоматизирована, вам стоит вести информацию о вашем сайте с его описанием, и программа сама разошлёт ваш сайт кому нужно, будь то 500 форумов, или 5000 номеров ICQ. Но знайте, поисковые системы этого не любят, а если вас заблокировали в поисковых системах, то при наборе «Сайт о собачках», пользователю, поисковая машина выдаст кучи сайтов, но только не ваш.

Друзья по тематике, тоже довольно таки хороший вариант, но в последнее время менее эффективный. Принцип таков, что вы ищите сайты похожей тематики. Например, ваш сайт о путешествиях, и вам нужно искать сайты такой же тематики, например тур-агенства, или заказ билетов для отдыха на берегу Красного моря, и так далее. Это тоже приносить пользователей, но, как правило, небольшой количество. Но вариант работает.

Каталоги. Добавление ссылки вашего сайта в каталоги, очень даже эффективный способ заявить о своём сайте. Огромное количество людей, которые ищут информацию в интернете, попадают на каталоги сайтов. Как правило, каталоги разбиты на категории, например: Зоология, автомобили, программы, бесплатное в сети, юмор, и т.д. И человек хочет найти сайты с анекдотами и заходит в раздел Юмор, где ваша ссылка уже присутствует, и он нажимает и выходит на ваш сайт. Есть кучи сайтов, которые помогают вам внести ваш сайт в каталоги. Есть такие понятия как «белые каталги», и «чёрные каталоги». Их отличие в том, что белые каталоги более популярны они известны всем поисковым машинам. То есть шанс прихода пользователей именно с «белых каталогов», куда выше, чем с так называемых «чёрных».

Поисковые машины, это программа настроена, искать информации в интернете и добавлять её в свою базу. Часто на форуме или на сайте, просматривая статистику посещений, вы видите, что сейчас в сети «Yahoo Bot», то есть интернет робот сайта Yahoo, вышел на ваш сайт в поисках новой информации, чтобы добавить её в базу, и после выдать эту информацию пользователю который задаёт запрос на поиск этой информации. Многие из нас так и не научились пользоваться поиском. Я расскажу немного о том, как

и что нужно спрашивать у поисковой машины, чтобы она выдала нам более или менее нужную нам информацию. Во первых если вы ищите сайт например государственный то знайте что почти все сайты государственные в России, имеют доменное имя типа gov.ru, или в Израиле gov.il, тоесть спрашивая у поисковой машины «Сайт министерства образования», добавьте через пробел в конце домен виде: «Сайт министерства образования gov.ru». Шансы на выдачу нужного сайта куда выше. Спрашивайте точно, а не в виде: «Личный сайт моего лучшего друга». Укажите имя вашего друга, фамилию, что-то, что заставило бы поисковую машину искать сайт с фамилией Иванов, а не Петров. То есть, задавая задачу поисковику, задайте ему как можно больше условий, и тогда результаты вашего поиска будут более точны. Например, вы ищите программу, не пишите поисковику: «Нужна программа для прослушивания музыки и если можно бесплатно». Куда правильнее будет написать: «Скачать бесплатно ауди-оплеер». Поисковик это не человек, который поймёт что вам нужно, это машина, которая идёт в свою базу, и ищет там, что-то похожее с вашим запросом.

Что такое домен и с чем его едят.

Доменные имена. О них можно отдельную книгу писать. Выше я уже описывал кратко что такое домен, хочу к этому вернуться:

*“Каждый подключённый к Интернету компьютерный сервер имеет собственный Интернет-адрес, который называется IP-адресом (*Internet Protocol*). Этот адрес состоит из четырёх разделенных точками чисел, каждое из которых имеет величину от 0 до 254.*

Конечно же, эти числа нелегко запомнить, а поэтому каждому IP соответствует уникальное имя домена. Серверы имен хранят списки, определяющие соответствие между именами и номерами.

Если при обращении к Интернету IP-адрес задается не в числовой форме, выполняется автоматическое обращение к серверам имен с целью отыскать IP-эквивалента для заданного вами имени домена.”

Другими словами домен это и есть адрес сайта, где вы пишете www.saitosobakah.ru. Домены бывают разные. Нет, не чёрные, белые и красные, а второго и третьего уровней.

Домен второго уровня – это домены которые ми чаще всего видим. Примеры таких доменов: .ru, .net, .com, .org, .info, .in, .name, .tv

2. Web **Мастерство**

Каждый домен, который вы видите в сети, имеет свой определенный смысл. Например, домен .ru – говорит о том, что сайт относиться к России (Russia). Домены .net, .org, .com, говорят о том, что это - Интернет, Организации, Коммуникации. Домен .tv – говорит о том, что сайт телеканала или чего-то связанное с телевидением. Например, в Украине много хостинговых компаний не регистрируют домен .ua, который относиться в Украине (Ukraine). Так как чтобы зарегистрировать такой домен, нужна справка о том, что вы являетесь главой компании или фирмы, завода, или чего ни будь в этом роде. С регистрацией доменов куча своих нюансов, в которые нужно войти, чтобы их понять.

Домены второго уровня – это домены которые имеют вид: .net.ru, com.ru, pp.ru, gov.ru, .org.ru, и того подобные. Такие доменные имена регистрируются чтобы подчеркнуть, что например: org.ru, говорит о том, что это Организация в России. Цены на регистрацию разные, каждый домен имеют свою цену, если она ниже у одних, то она выше у других. Каждые делают на этом свою копейку. Лучше регистрировать у официальных регистраторов, так надёжнее и дешевле.

Хостинг и всё о нём.

Хостинг, с англ. (Hosting - от слова Host). Существует несколько способов опубликовать вашу информацию в Интернете. Первый и самый простой - воспользоваться тем дисковым пространством, которое провайдер предоставляет бесплатно (большинство провайдеров при подключении через них бесплатно дают 5-10 Мб). Для "домашней странички", прайс-листа и тому подобных вещей этого места вполне хватит. Есть только один минус - адрес такой странички будет выглядеть как-то вроде http://www.site.ru/guest/newbe/index.html. Запомнить, продиктовать по телефону или перепечатать набранный на визитке подобный адрес довольно сложно. Кроме того, вместо того, чтобы рекламировать вашу фирму или говорить о вашем хобби такой адрес, в первую очередь, рекламирует вашего провайдера... Это не означает, что пользоваться такими адресами нельзя - они вполне годятся для многих нужд. Как бумага, в клеточку вырванная из тетради. На ней удобно делать пометки для себя, написать записку жене и т.п., но вот использовать ее для "фирменных" писем как-то не принято...

Следующая возможность - это создание "домена третьего уровня". Выглядит такой адрес как "http://ваше имя.provider.ru" и значительно легче запоминается, диктуется и т.п. Домены третьего уровня довольно часто можно получить бесплатно или за очень маленькие деньги все у того же провайдера или на каком-нибудь сервере, предоставляющем бесплатный хостинг, например, на chat.ru.

2. Web **Мастерство**

Кстати, вопрос о том, что предпочесть: бесплатный хостинг или хостинг у вашего провайдера тоже имеет некоторое значение. По большому счету, у бесплатного хостинга преимущество только одно: ваш адрес не будет меняться при смене провайдера. Это достаточно важно, т.к. в большинстве случаев ваши посетители находят вас через поисковые системы или, глядя на визитку, которую вы дали, может быть, год назад. Если за это время вы сменили провайдера, то потенциальный посетитель увидит сообщение о том, что "документ не найден" и пойдет к вашим конкурентам. Однако бесплатные хостеры тоже хотят кушать, поэтому в качестве платы за предоставление места требуют от вас разместить их баннеры на своих страницах или даже размещают их автоматически. Кроме того, бесплатный хостер не гарантирует непрерывную работу - в любой момент он может "закрыться на ремонт", что-то поменять в конфигурации и т.п. Я уж не говорю о том, что выкладывать файлы к своему провайдеру намного проще - соединение с сервером почти прямое и, соответственно, наиболее быстрое.

Тут стоит подумать о редиректорах. Это такая штука, которая автоматически "перебрасывает" вашего посетителя с одного адреса на другой. Есть специальные службы, которые этим занимаются, например da.ru или attend.to. Зарегистрировавшись в такой службе, и указав ваш текущий адрес, вы сможете публиковать свой адрес в виде http://attend.to/ваше_имя или http://ваше_имя.da.ru и пользователь будет автоматически перенаправлен на ваш текущий адрес. А при смене провайдера вам надо будет всего лишь зайти на сайт и изменить свой текущий адрес.

Дальнейшее развитие сайта требует регистрации собственного "домена второго уровня", при котором ваш адрес в Интернете выглядит как www.ваше_имя.ru Это делается тоже сравнительно несложно и недорого - типичная стоимость это 35 долларов в год за регистрацию имени и 10 долларов в месяц за место на диске и поддержание сервера. При этом при переходе к другому провайдеру ваш адрес сохраняется, просто данные физически переносятся на другой сервер. В абсолютном большинстве случаев для такого хостинга, достаточно виртуального сервера (это когда на одном компьютере расположено несколько сайтов с разными именами), но если ваш сайт будет слишком большим или "излишне популярным", то через некоторое время придется задуматься о собственном выделенном сервере.

По большому счету, разница между виртуальным и выделенным сервером не очень велика и проявляется только в том случае, если вам надо делать что-то относительно нестандартное, например, запускать долго-работающие или сильно загружающие

процессор скрипты. Кроме того, плюсом выделенного сервера является то, что вы получаете над ним полный контроль - в любой момент вы можете доставить те программы, которые вам нужны, изменить конфигурацию и т.п. Правда, абсолютному большинству сайтов это не требуется...

Все сказанное выше - это теория, в которой, как обычно, все гладко. Теперь немного практики.

Физическое расположение сервера имеет довольно существенное значение, особенно если ваш сайт занимает много места. Чем ближе к вам расположен сервер, тем быстрее связь и тем проще его обновлять. Если же сервер расположен с вами в одном городе, то в случае крупных обновлений вы сможете банально приносить данные на винчестере. Скорость связи с сервером можно посмотреть с помощью команды ping, а "расстояние" с помощью команды tracert. Обе эти команды уже есть в Windows, а открыв окно ДОС и набрав "ping /?" или "tracert /?" вы узнаете как ими пользоваться.

Эти же данные влияют и на то, насколько удобно будет вашим пользователям смотреть ваш сайт. Поэтому стоит оценить, какие пользователи для вас приоритетны (по географическому положению) и размещать сервер так, чтобы для них он был "поближе". Например, если вы ориентируетесь на "буржуев", то имеет смысл и хостинг организовывать там же, тем более, что цены везде примерно одинаковы.

При смене провайдера имеет смысл договариваться с ним о том, чтобы несколько месяцев он подержал на вашем старом адресе страничку с извещением о том, что вы "переехали" и с новым адресом. Можно и автоматический редирект сделать, это легко прописывается в META тэге странички. Следует учитывать и то, что изменится и ваш почтовый адрес. Здесь - то же самое, договоритесь о перенаправлении почты. Это. разумеется, будет стоить каких-то денег, но "непотеря" клиентов, я думаю, их окупит.

При выборе хостера стоит не полениться и посмотреть разные варианты. Обязательно поинтересуйтесь возможными ограничениями на трафик (количество переданных/принятых данных), на размер сайта, на загрузку сервера (например, многие провайдеры ограничивают максимальное время выполнения скрипта и суммарное время выполнения всех ваших скриптов) и т.п. Узнайте, можно ли устанавливать свои скрипты,

предоставляет ли хостер набор готовых CGI, какие программы и языки установлены на сервере, есть ли telnet доступ, можно ли заводить собственные домены третьего уровня, можно ли заводить собственные почтовые ящики и сколько, автоответчики и т.п. Спрашивая про ограничения трафика и услышав "неограничено" в ответ, поинтересуйтесь, что значит "не ограничено" и какой цифрой оно выражается. Если же ограничения есть, то узнайте, сколько будет стоить их превышение. Учтите, что те вещи, которые сейчас вам кажутся незначительными, например, наличие базы данных или поддержка PHP могут вам понадобиться, довольно скоро - сайт-то будет развиваться и захочется чего-то нового... А смена хостера в реальной жизни - это как минимум неделя нервотрепки и неустойчивой работы сервера...

За статью спасибо сайту Codenet

Языки программирования в WEB.

Языки веб-программирования, что это такое.

Вы где-то там читали, что для того, чтобы сделать гостевую книгу или опрос, нужно знать какое-то там веб-программирование. Вы когда-то там слышали, что такое веб-программирование. Вот мы и встретились, ведь я когда-то тоже мучился этими вопросами, а ныне попытаюсь дать на них ответы.

Языки веб-программирования - это соответственно языки, которые в основном предназначены для работы с интернет-технологиями. А некоторые и создавались только для работы с каким-нибудь ресурсом, и лишь долгое время спустя к ним приходила известность и всеобщее признание (например, PHP). Но я не буду углубляться в историю создания различных языков веб-программирования, поскольку не она является предметом этой статьи, а если читателю интересно, он может найти её на сайтах разработчиков.

Языки веб-программирования делятся на две группы: клиентские и серверные. Напомню, что такое сервер: это и тот компьютер, где хранится ваш сайт, и та программа, которая обрабатывает запросы браузера к какой-либо странице.

2. Web **Мастерство**

Клиентские языки

Как следует из названия, клиентские языки обрабатываются на стороне клиента пользователя, а если проще - программы на клиентском языке обрабатывает браузер. Отсюда следует и недостаток – это то, что обработка скрипта зависит от браузера пользователя, и пользователь имеет полномочия настроить свой браузер так, чтобы он вообще игнорировал написанные вами скрипты. При этом, если браузер старый, он может не поддерживать тот или иной язык или версию языка, на которую вы опираетесь. С современными браузерами таких проблем возникать не должно, к тому же языки программирования не так уж часто кардинально обновляются (раз в несколько лет) и лучшие из них давно известны. Также код клиентского скрипта может посмотреть каждый, выбрав в меню “Вид” своего браузера вкладку “Исходный код” (или что-то в этом роде).

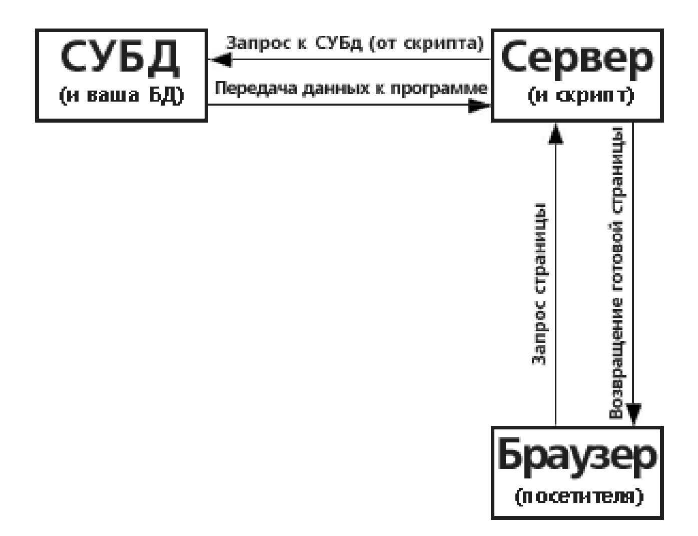
Преимущество же клиентского языка заключается в том, что обработка скриптов на таком языке может выполняться без отправки документа на сервер. Это легче объяснить на примере: Допустим, вам надо проверить правильно ли пользователь ввел e-mail (т.е., например, проверить в нем наличие “@”); чтобы это сделать пользователю, надо было бы отправить форму с заполненными данными, потом дождаться, пока она обработается, и лишь после этого получить сообщение об ошибке (если она, разумеется, присутствует). Процесс слишком долгий. С клиентским же языком программа сразу проверит правильное заполнение формы перед отправкой, и, если необходимо, выведет ошибку. Отсюда же вытекает ограничение, что с помощью клиентского языка программирования ничто не может быть записано на сервер, то есть, например, с его помощью нельзя сделать гостевую книгу, потому, что тогда надо записывать сообщения в какой-либо файл на сервере.

Самым распространенным из клиентских языков является JavaScript, разработчиками которого является компания Netscape (www.netscape.com, думаю, вам известен их браузер Netscape Navigator) совместно с компанией SunMicrosystems (www.sun.com). Другой вариант клиентского языка это, например, VisualBasicScript (VBS). Чтобы начать учить клиентский язык веб-программирования, Вам понадобится поддерживающий этот язык браузер (Internet Explorer (www.microsoft.com), Opera (www.opera.com), Netscape Navigator (www.netscape.com), Mozilla (www.mozilla.org), будут подходящими вариантами (лично я пользуюсь последним)) и обучающий материал, который можно найти на сайте alepira.ural.ru

2. Web **Мастерство**

Серверные языки

Итак, теперь разберемся в том, как обрабатываются скрипты на серверном языке программирования. Для начала предоставлю следующую схему:



Когда пользователь дает запрос на какую-либо страницу (переходит на нее по ссылке, или вводит адрес в адресной строке своего браузера), то вызванная страница сначала обрабатывается на сервере, то есть выполняются все скрипты, связанные со страницей, и только потом возвращается к посетителю в виде простого HTML-документа (то есть посетитель уже никак не сможет увидеть код Вашего скрипта). Но работа ваших скриптов уже полностью зависима от сервера, на котором расположен ваш сайт, и от того, какая версия того или иного языка поддерживается хостингом.

Серверные языки программирования открывают перед программистом большие просторы в деятельности, однако, сколько бы не писали люди, продвигающие язык, что их язык очень легок для обучения, без предварительного груза знаний освоить довольно-таки тяжело.

Здесь же стоит упомянуть, что такое Система Управления Баз Данных, или СУБД. Это, по сути, тоже сервер, на котором в определенном пользователем порядке хранится разная необходимая информация, которая может быть вызвана в любой момент. Это библиотека, в которой все материалы аккуратно сложены по полочкам и в любой момент могут быть взяты. Обычно при покупке хостинга выделяется одна База данных (БД), в которой пользователь может создавать множество таблиц, а в них уже хранить разнообразную информацию. То есть если опять же вернуться к примеру с гостевой книгой, то в какой-либо созданной Вами таблице можно хранить сообщения, оставленные пользователями. Можно, конечно, хранить их и в текстовом файле, но это менее надежно, да и к тому же, я привел лишь мелкий пример, а если, скажем Вам надо хранить

пароли (а их надо хранить в зашифрованном виде), или связать несколько таблиц при обращении к каким-либо данным, тут без БД не обойтись.

В настоящее время стали известны и не напрасно СУБД, обращение к которым производится посредством Structured Query Language (SQL), или структуризированным языком запросов. Чтобы работать с этими базами данных (дополнять, обновлять, делать запросы и т. д.) вам необходимо знать этот самый SQL. Среди таких СУБД наиболее известна MySQL (www.mysql.com), я же для себя предпочел PostgreSQL (www.postgresql.org).

Пара слов напоследок

Если продолжать говорить о языках программирования, то сейчас существуют языки, которые встраиваются в сам документ, и те программы, на которых надо предварительно компилировать, то есть превращать, написанные вами исходные коды в готовую программу; недостаток вторых заключается в том, что если вам нужно обновить скрипт, то придется заново компилировать дополненные коды.

Среди серверных языков программирования, выделяются PHP: (PHP: Hypertext Preprocessor) (www.php.net), Perl (www.perl.com), SSI (Server Side Include). Для тестирования этих скриптов, Вам понадобится уже по больше: сервер (www.apache.org), интерпретатор языка (можно взять на сайте производителя), ну и конечно при продуктивной работе еще и СУБД.

Обучающие доки можно найти на следующих ресурсах:

- PHP, SQL, Perl - www.opennet.ru/docs/
- PHP, Perl, MySQL- http://www.dklab.ru/map/
- Обучение SQL - http://docs.luksian.com/db/sql/sql-prim/
- JavaSrcipt 1.4 - http://alepira.ural.ru/servguide14/index.htm
- Книга по PostgreSQL- http://www.intermedia.net/support/sql/sqltut.asp
- Ещё один учебник по PostgreSQL - http://www.commandprompt.com/ppbook/

Ну и другие связанные ресурсы:

- PHP по русски - http://php.spb.ru/
- PHP клуб (Новости, форум, и т.п.) - http://www.phpclub.com/
- Perl в России - http://perl.org.ru:8000/documentation/
- Perl6 в Интернет - http://www.perl6.ru/

За статью огромное спасибо сайту Постройка.

3. **Хакерство и безопасность в сети.**

Что такое антивирус, и что он умеет.

Обычно антивирусы сканируют ваше рабочее пространство, такое как носители памяти, Интернет, электронную почту на предмет вирусов. При нахождении оного антивирус проводит с ним комплекс мероприятий по обезвреживанию. Антивирус – незаменимая вещь для каждого уважающего себя пользователя компьютера.

Антивирус Касперского 7.0



Самый популярный антивирус среди русскоязычного пространства и не только. В народе его прозвали самым хрюкающим антивирусом за его звук при нахождении зараженного файла. Новый антивирус версии 7.0 радует новыми возможностями. Введена трёхступенчатая защита известных и новых Интернет-угроз.

1. Стандартная проверка по базам, т.е. антивирус, сверяет содержимое файла со своими базами и если находит соответствие – то там вирус. Тут всё понятно.
2. Эвристический анализатор. Антивирус, используя собственные «мозги» вычисляет вирус по возможному коду. Эта функция помогает искать вирусы, не занесённые в базы.
3. Поведенческий блокиратор. Антивирус внимательно следит за программами, которые разместились на вашем компьютере, и вычисляет всех тех, кто ведёт себя недостойно, как вирус.

3. **Хакерство и безопасность в сети.**

Радует обилие дополнительных возможностей, таких как наличие средства создания диска для аварийного восстановления системы. Обеспечивая надёжную защиту, этот антивирус потребляет достаточно большое количество системных ресурсов. Поэтому если вы испытываете нехватку системных мощностей, то вряд ли работа с этим антивирусом покажется вам комфортной.

Так же можно приобрести антивирус в пакете Касперский Internet Security 2007, который будет защищать вас ещё и от прямых атак из Интернета. Но такой пакет будет стоить уже 1600р. за год использования.

Dr.Web (**Доктор Веб**)

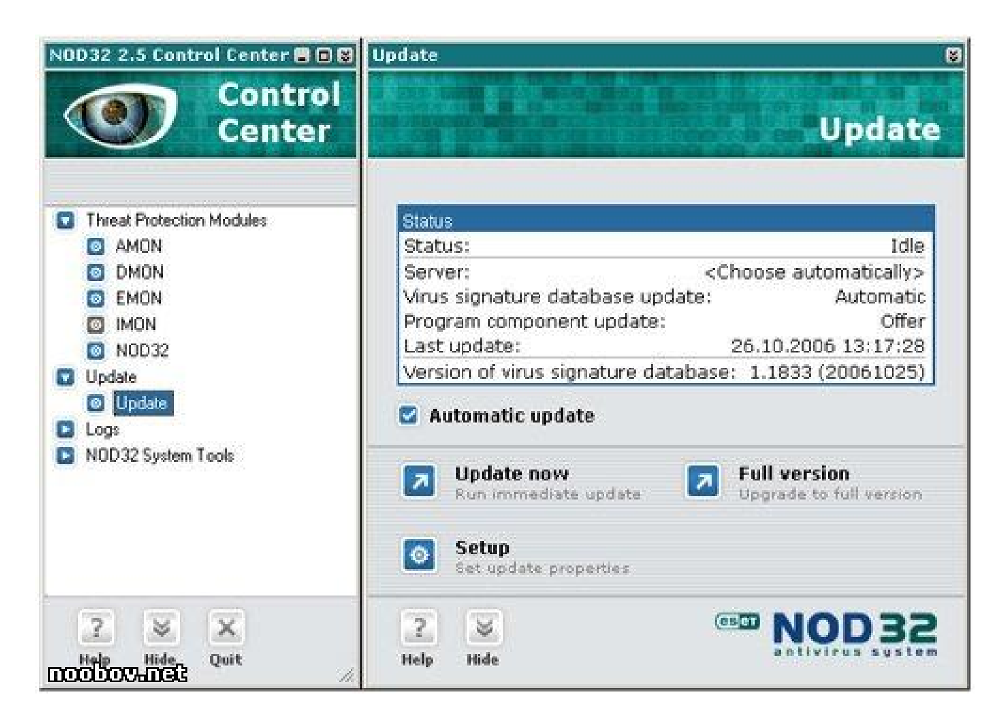


Этот антивирус является вторым по известности в России. Мелкие неприятности, возникающие при работе с ним (несколько паучков висящих в системном трее), невозможность автономной установки без подключения к Интернет с лихвой компенсируются его сканирующими возможностями. Доктор Веб обеспечивает хорошую защиту вашего компьютера от вирусных атак.

Также преимуществом можно назвать относительно малое потребление системных ресурсов и небольшой размер обновлений. Годовая лицензия на один компьютер стоит около тысячи российских рублей.

3. **Хакерство и безопасность в сети.**

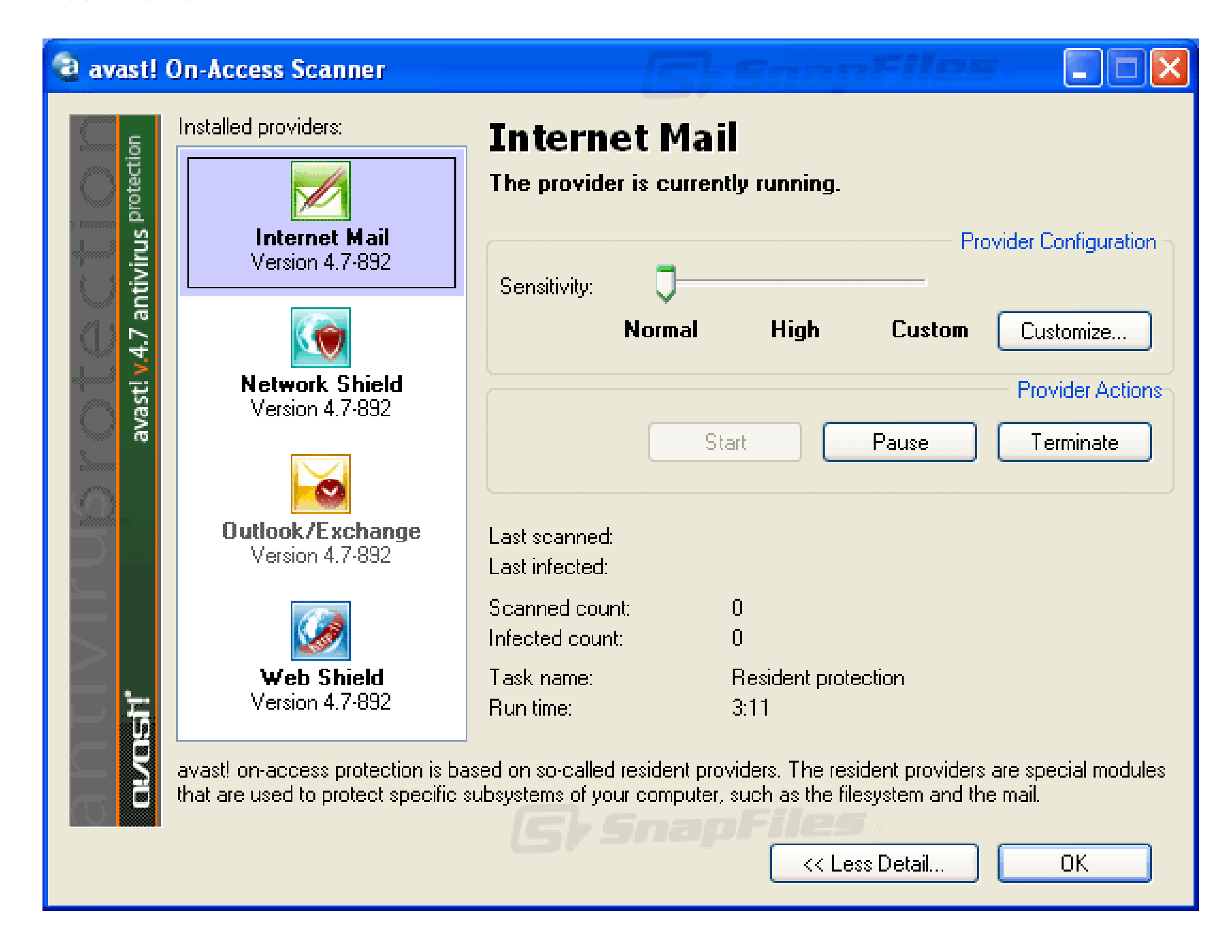
Nod 32



Этот антивирус созданный иностранной компанией ESET является одним из лидеров среди антивирусного программного обеспечения. Только Nod 32 может похвастаться, что на протяжении уже семи лет подряд показывает при тестировании высокую эффективность нахождения вирусом, а именно этот показатель у него ближе остальных антивирусов к 100%. Кроме того Nod 32 отличается высокой скоростью работы, обладает всеми современными средствами защиты компьютера. В наличии довольно приятный интерфейс, возможность частых обновлений, множество функций, реализованных на довольно высоком уровне. Предоставляется ознакомительная версия сроком 30 дней. Также в плюсы можно занести наличие русской версии программы.

3. **Хакерство и безопасность в сети.**

Avast! Home



Кроме вышеописанных платных антивирусов существуют и вполне достойные представители среди бесплатного софта. Одним из таких решений является антивирусный пакет Avast. Почему же из всех бесплатных антивирусов я выбрал именно этот? Вариация для домашних пользователей (именно она является бесплатной) включает в себя все модули и функции, защищая вас не только от вирусов, но и от различных шпионов, контролируя вашу электронную почту, ICQ, и другие пространства в которых могут завестись вирусы. Почему это можно назвать плюсом? Обычно версия для домашних пользователей является сильно урезанной в функциях и возможностях. Но в случае с

Avast! Home бесплатная версия сохраняет свою функциональность. Также этот пакет обеспечивает довольно неплохую защиту (не самую лучшую, но всё же) и сам по себе является довольно оригинальным антивирусом с множеством полезных функций, таких как создание резервных копий файлов, на случай краха системы.

Сама программа похожа на плеер, в ней даже присутствует поддержка скинов, а также есть мультиязычный интерфейс, в который включен русский язык. Да и скажу по секрету, что автор выбирает именно этот антивирусный пакет.

3. **Хакерство и безопасность в сети.**

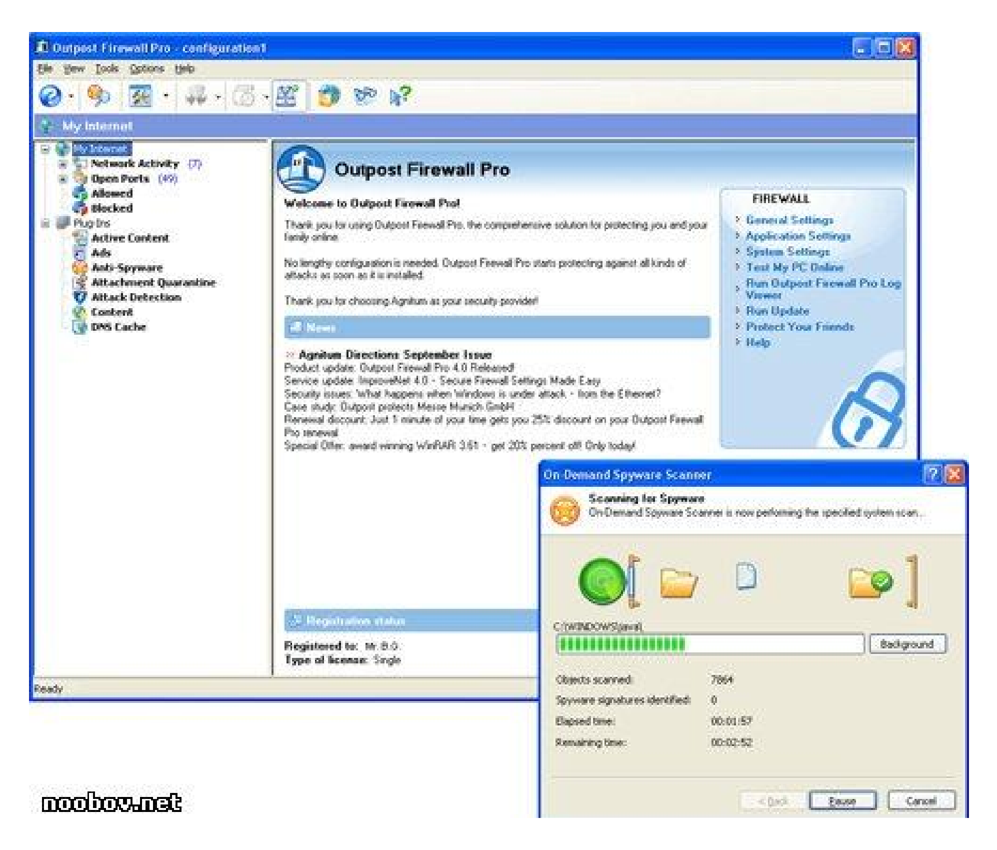
Существует также несколько бесплатных антивирусных программ, обеспечивающих вполне неплохую защиту, на уровне лучших платных решений, но обеспечивающих только сканирование, например, дискового пространства, оставляя незащищенной почту, Интернет-трафик. Поэтому, для того, чтобы обеспечить безопасность нужно будет установить вдобавок ещё кучу программ. Что, согласитесь, нерационально. Поэтому такие программы в своём обзоре я оставлю без внимания.

Файерволы

Файервол предназначен для контроля входящих и исходящих Интернет-соединений. Он не даёт подключиться к вашему компьютеру какому-нибудь непрошенному гостю, а также передать сведения, накопленные троянцем. Вы можете закрыть доступ обновлению Windows или другим программам, которые непрошено кушают ваш трафик.

Более-менее надёжную защиту даёт стандартный файервол Windows (присутствует в Windows XP sp2, а также в Vista). Но если вы хотите защиту посерьёзней, то я порекомендую вам единственное, но очень мощное и главное бесплатное решение - Agnitum Outpost Firewall. Использовать что-нибудь другое я порекомендую лишь в том случае, если вы покупаете комплексный пакет антивирус + файревол от какой-нибудь одной компании, например Касперский Internet Security.

Agnitum Outpost Firewall



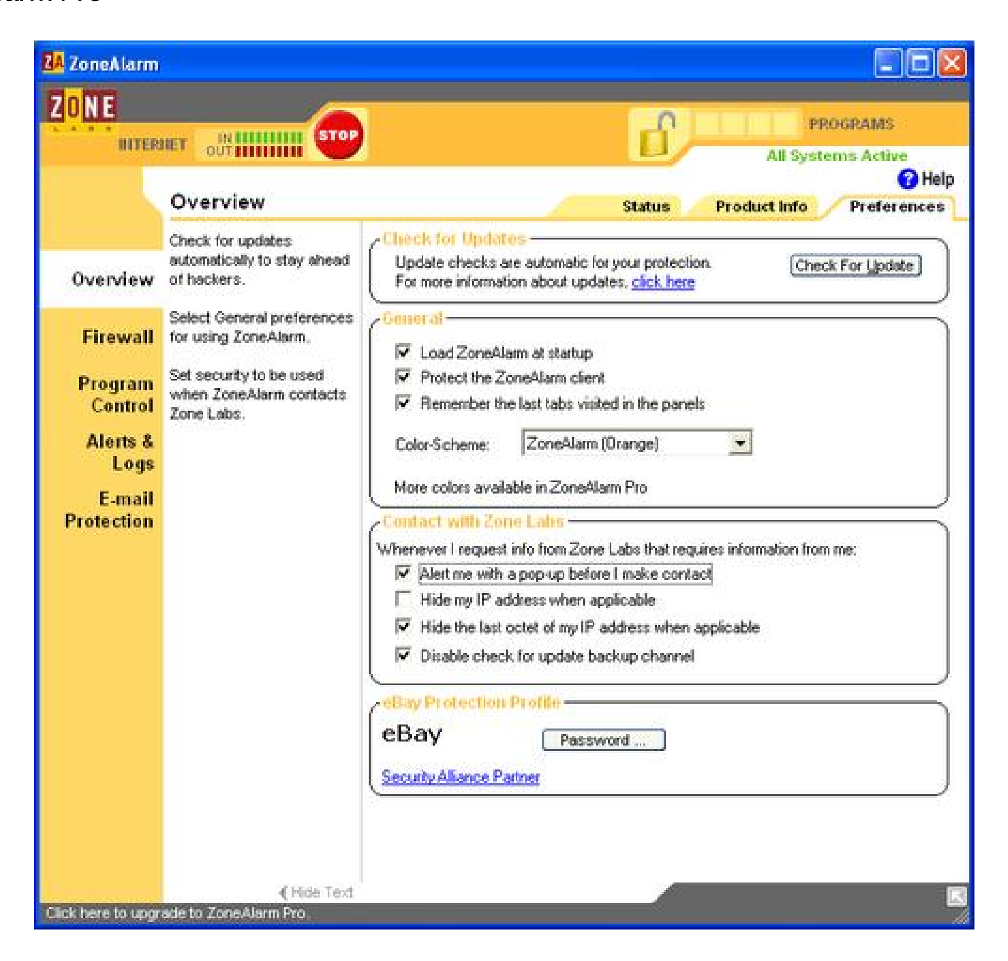
3. **Хакерство и безопасность в сети.**

Outpost Firewall – это персональный файервол, проще говоря – программа для защиты компьютера от хакерских атак из Интернета. Кроме этого, Outpost обеспечивает блокировку загрузки рекламы и активного содержимого веб-страниц, а тем самым – и ускорение работы в Интернете.

Существует также режим автообновления, поэтому не обязательно скачивать новые и новые версии. Но будьте осторожны. Если вы не очень разбираетесь в компьютерах, плюс рядом нет человека, способного вам помочь или подробной инструкции по настройке, то с установкой файервола вам следует повременить, иначе вы рискуете остаться без Интернета и локальной сети, так как всё это будет заблокировано.

Помимо бесплатной версии существует и профессиональная, то есть платная. Она обладает значительно большими настройками. Но всё же если вы работаете в домашних условиях, то вам с лихвой хватит бесплатного варианта.

ZoneAlarm Pro



ZoneAlarm Pro – это ещё один популярный файрвол. Кроме основных функций файрвола он может контролировать исходящие данные и пресекать отправку нежелательной информации по почте или через web-интерфейс. ZoneAlarm контролирует входящую и

исходящую почту. Файервол может удалять с посещаемых страниц рекламу, экономя трафик и уменьшая время загрузки страниц. Блокировка скриптов и активного

содержимого поможет предотвратить заражение компьютера при посещении определенных веб-сайтов. К сожалению, программа не имеет русскоязычного интефейса.

Sunbelt Kerio Personal Firewall

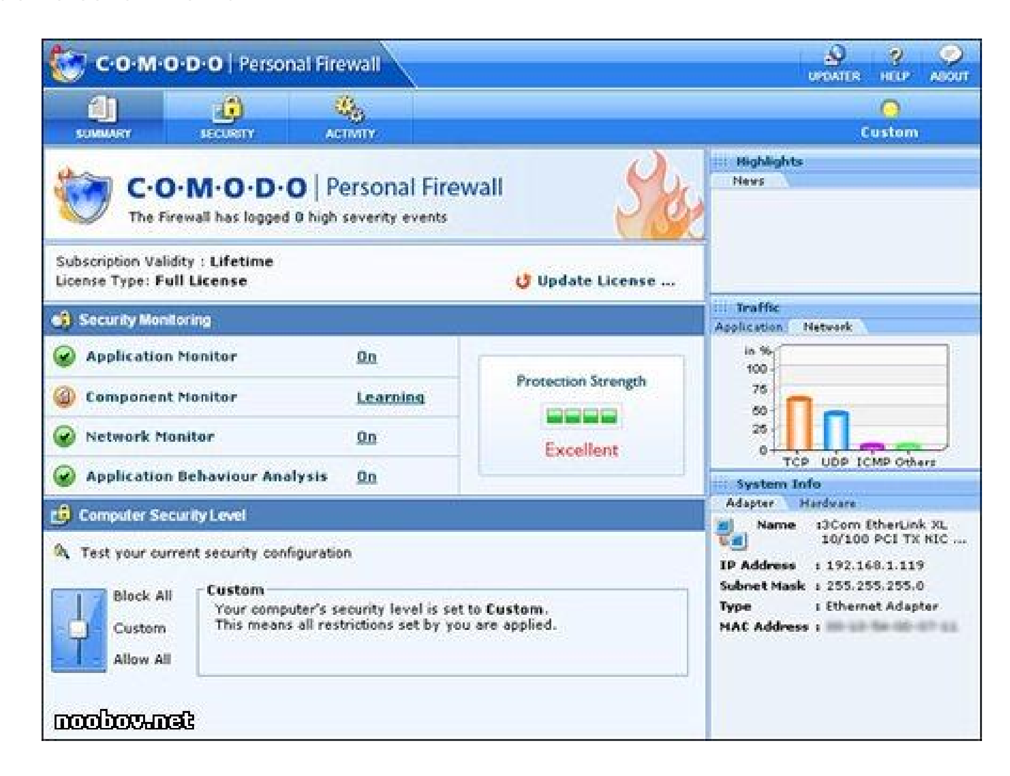


Эта программа является также популярным решением в защите подключений вашего компьютера. Sunbelt Kerio Personal Firewall отслеживает активность работающих через Интернет программ, позволяя разрешить или запретить тому или иному приложению доступ в Сеть. Для большей гибкости настройки предусмотрена установка временных интервалов, когда будут действовать отдельные правила. Кроме этого, выдает сообщение о попытке соединения или сканировании портов компьютера.

Выгодное отличие этой программы довольно простая настройка. В остальном, сильных отличий от программ аналогов этот файервол не имеет. Программа платная, без оплаты работает 30 дней в полнофункциональном режиме. Есть русский интерфейс.

3. **Хакерство и безопасность в сети.**

Comodo Personal FireWall



Ещё один качественный файервол с простым интерфейсом. Поможет защитить ваш компьютер от троянов и хакерских атак. Из положительных особенностей – нетребовательность к ресурсам компьютера и малый размер. Идеален для маломощных компьютеров.

В этом обзоре мы рассмотрели самые популярные программы, обеспечивающие защиту вашему компьютеру. В обзоре присутствуют как платные, так и бесплатные варианты программ. Стоит ли покупать софт или обходиться бесплатными вариантами, которые далеко не всегда уступают по качеству платным аналогам – решать вам. НюБоВ.НеТ только показывает верную дорожку – а идти по ней приходиться вам самим. Удачи в пути!

Я хочу стать хакером.

Конечно же, каждый из нас хоть раз хотел стать настоящим хакером. И конечно же, мы не часто задумываемся, чем это может для нас обернуться. Но в принципе для расширения знаний побаловаться немного можно и даже полезно. Ниже немного хочу рассказать, откуда же взялось слово Хакер, и что, из себя представляет данная «Профессия».

3. **Хакерство и безопасность в сети**.

ХАКЕР — квалифицированный компьютерный взломщик, злоумышленник, специализирующийся на поиске и использовании несанкционированного доступа в вычислительные сети или другое компьютеризированное оборудование для незаконного получения информации, извлечения выгоды, нанесения ущерба.

Профессия — хакер. Компьютерный андеграунд созрел.

"Ведомости". 22.09.2004, №172 (1212)

Значительную часть хакеров и вирусописателей составляют ориентированные на прибыль профессионалы. К такому выводу пришли эксперты антивирусной компании Symantec. В российских фирмах по компьютерной безопасности соглашаются, что деятели андеграунда уже научились считать и зарабатывать деньги.

Опубликованный вчера отчет Symantec по безопасности в Интернете за первое полугодие 2004 г. констатирует, что вирусы взяли на вооружение спамеры и злоумышленники, крадущие личную информацию, например номера кредитных карт. А хакеры предпочитают атаковать небольшие компании, занимающиеся интернет-коммерцией, говорится в отчете.

“Идет переориентация на коммерческие интересы, — сказал газете The Wall Street Journal старший директор инженерного подразделения службы реагирования Symantec Элфред Ньюджер. — Я думаю, мы во многих случаях имеем дело с профессиональными разработками компьютерных программ”. По данным Symantec, в первом полугодии 2004 г. компьютеры под управлением Windows в Интернете пережили 4496 атак — в четыре раза больше, чем за аналогичный период прошлого года. Если атаки вирусов в прошлые годы просто мешали работе Интернета, то теперь они предназначены для создания сетей зараженных компьютеров, через которые злоумышленники рассылают спам или устраивают атаки на корпоративные серверы.

Вирусописатели стали быстрее реагировать на появление новых возможностей. Если в прошлом году, по данным Symantec, среднее время от обнаружения “бреши” в компьютерной программе до появления использующей ее вредоносной программы составляло 99 дней, то в первом полугодии 2004 г. оно сократилось до 5,8 дней.

Российские компании, работающие в области компьютерной безопасности, соглашаются с выводами Symantec. В компьютерный андеграунд профессионалы пришли еще в конце прошлого десятилетия, считает менеджер по корпоративным коммуникациям “Лаборатории Касперского” Алексей Зернов. Если в эпоху “хулиганского вирусописательства” программы были нацелены на максимальный и наиболее эффектный урон пораженной системе, то теперь они действуют незаметно и не вредят личным данным пользователя, рассказывает он. “Вирусы сейчас делают так, чтобы пользователь последним узнал о заражении своего компьютера”, — признает

Зернов. Он вспоминает, что 15 лет назад антивирусные базы достаточно было обновлять раз в месяц, пять лет назад — раз в неделю, а сейчас это необходимо делать 2-3 раза в день.

“Хакеров мы, конечно, в лицо не видим, — говорит управляющий партнер компании "Ашманов и партнеры" Игорь Ашманов, — но иллюзия о том, что они прыщавые подростки, неверна”. Ашманов считает, что рынок спамерских рассылок демонстрирует признаки зрелости. Например, уже сложилось разделение труда между группировками — одни разыскивают адреса электронной почты, другие ищут хостинг-провайдеров для рассылки спама.

Впрочем, с ростом коммерциализации и профессионализма в компьютерном андеграунде согласны не все эксперты. “Если люди воруют деньги так, что об этом знает даже Symantec, — ехидничает хакер, пожелавший сохранить анонимность, — то это не профессионалы”. Вопрос о деньгах всегда был

актуальным для хакеров, уверен директор департамента информационной безопасности “УСП Компьюлинк” Владимир Ляшенко. Но он признает, что хакерские технологии становятся все более изощренными и дорогими. (использованы материалы WSJ)

Я всегда подвергаюсь атакам со стороны хакеров.

Некоторые из нас неоднократно подвергались атаке со стороны хакеров. Существуют различные виды атак. Это может быть атака именно на ваш компьютер, или атака на ваш сайт, атака на вашего провайдера, локальную сеть, и т.д. Но не всегда мы знаем как бороться с таким явлением.

Самая популярная в наши дни атака:

DoS-**атака** (от англ. Denial of Service — «отказ в обслуживании») и DDoS-атака (Distributed Denial of Service — «распределённый отказ обслуживания») — это разновидности атак злоумышленника на компьютерные системы. Целью этих атак является создание таких

условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

Существуют различные причины, по которым может возникнуть DoS-условие:

Ошибка в программном коде, приводящая к обращению к неиспользуемому фрагменту адресного пространства, выполнению недопустимой инструкции или другой

необрабатываемой исключительной ситуации, когда происходит аварийное завершение серверного приложения. Классическим примером является обращение по нулевому (англ. null) указателю.

Недостаточная проверка данных пользователя, приводящая к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов (исчерпанию процессорных ресурсов) либо выделению большого объема оперативной памяти (исчерпанию памяти).

Флуд (англ. flood) — атака, связанная с большим количеством обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию, имеющая своей целью или приведшая к отказу в работе системы из-за исчерпания ресурсов системы — процессора, памяти либо каналов связи.

Атака второго рода — атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса.

Если атака (обычно флуд) производится одновременно с большого количества IP-адресов, то в этом случае она называется распределённой атакой на отказ в обслуживании (DDoS).

Защита от DoS-атак

Меры противодействия DoS-атакам можно разделить на пассивные и активные, а также на превентивные и реакционные.

Ниже приведён краткий перечень основных методов.

Предотвращение. Профилактика причин, побуждающих тех или иных лиц организовывать DoS-атаки. Очень часто атаки являются следствиями личной обиды, политических, религиозных разногласий, провоцирующего поведения жертвы и т. п.

Фильтрация и блэкхолинг. Эффективность этих методов снижается по мере приближения к цели атаки и повышается по мере приближения к её источнику.

Устранение уязвимостей. Не работает против атак типа флуд, для которых «уязвимостью» является конечность тех или иных ресурсов.

Наращивание ресурсов.

Рассредоточение. Построение распределённых и продублированных систем, которые не прекратят обслуживать пользователей даже если некоторые их элементы станут недоступны из-за атаки.

Уклонение. Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью.

3. **Хакерство и безопасность в сети**.

Активные ответные меры. Воздействие на источники, организатора или центр управления атакой. Меры могут быть как технического характера (не рекомендуется), так и организационно-правового характера.

Вирусы, шпионы, и трояны.

Многие из нас конечно же знают такие термины как: *Вирус, Троян*. Но немногие из нас имеют представление о том, какая между ними разница, и какую функцию выполняет каждый из них. Давайте рассмотрим, что же такое «Вирус».

Вирус (Червь) –это любая компьютерная программа, способная размножаться и наносить вред пользователям. Такая программа, попав в один компьютер, способна заразить множество других, особенно если зараженный комп подключен к локальной сети. По Интернету вирус предается от зараженного компьютера через электронную почту (особенно опасны незнакомые прикрепленные файлы). Можно принести вирус на дискете и так далее, и так далее. Вирусы проявляются по-разному. Наиболее безобидные сами перезагружают ваш компьютер или выдают сообщение, что жесткий диск отформатирован. А могут ведь и вправду отформатировать, или хотя бы стереть файлы (нужны они вам или нет, вирус не волнует). Совсем злобные вирусы могут украсть номер вашей кредитной карточки со всеми вытекающими последствиями.

Троян – это вредоносная программа, замаскированная под обычное приложение. Название взято из античной легенды о троянском коне. Данная программа после запуска, работает по одному принипу, своровать информацию с вашего компьютера. Ей неинтересно перезагрузка вашего компьютера, её интересуют файлы с определёнными разрешениями. Она знает что воровать, и кому отправлять наворованное. Такие программки могут быть незаметны, и запускаться даже когда вы выходите на какой либо сайт. (В случае если сайт инфицирован). Известных троянов кучи, лично на моей практике часто встречался всеми известный троян Pinch. Его версия дошла до отметки 3.0, и сайт разработчиков был закрыт. Принудительно или нет, знать нельзя.

Агентство The Associated Press назвало восемь самых известных вирусов, написанных за последние 25 лет. Первым глобальным компьютерным вирусом признан ELK CLONER (1982), который заражал компьютеры Apple II и распространялся на дискетах.

Первым вирусом для DOS составители списка называют BRAIN (1986), написанный двумя братьями из Пакистана. Вирус выводил на экран зараженного ПК телефон принадлежащей братьям мастерской по ремонту компьютеров.

3. **Хакерство и безопасность в сети**.

MORRIS (1988) стал первым действительно масштабным вирусом, заразившим более 6000 компьютеров военных и университетских компьютеров, подключенных к интернет. Вирус Melissa, появившийся в 1999, первым начал использовать для распространения электронную почту. А Love Bug в 2000 первым начал использовать для распространения особенности человеческой психологии, успешно маскируясь под “письмо любви”.

Созданный в 2001 Code RED уже не требовал от пользователя никаких действий – чтобы заразиться, достаточно было подключиться к интернету без использования файрвола. Вирус эксплуатировал известную “дыру” в ПО Microsoft, которую, однако, многие пользователи не спешили закрывать заплаткой. Другим вирусом, вызвавшим столь же массовую эпидемию, оказался Blaster (2003 год).

Ну а самым масштабным, по мнению AP, был ущерб от эпидемии вируса Sasser и его модификаций в 2004 году. Написанный 18-летним немцем червь вызывал постоянные перезагрузки компьютера и сумел заразить более миллиона компьютеров по всему миру. Модель распространения этого вируса также подразумевала использование незакрытых дырок в ПО.

Нынешние интернет-эпидемии, отмечают составители, менее масштабны – пользователи понемногу привыкают к постоянным обновлениям используемого программного обеспечения, а часть вирусов отсекается провайдерами на аппаратном уровне, не позволяя локальной эпидемии перерасти в мировую.

Хочу так же немного рассказать и о троянах, и принципах их работы. Вот некоторые основные виды троянов:

Back Door. Состоит из клиента и сервера. Сервер отправляется жертве и в дальнейшем вся работа ведется по принципу клиент-сервер, т.е. злоумышленник посылает команды через клиента, а сервер их выполняет. В зависимости от настойки сервера и трояна вы можете ограничить доступ к серверу паролем или поставить определенное количество человек подключенных в одно время к серверу. После подключения к серверу вы можете управлять компьютером точно также как и своим: перезагружать, выключать, открывать CD-ROM, удалять, записывать, менять файлы. Также можно вытаскивать пароли. В общем,

функций миллион, но также все зависит от самого трояна, например Sub7 имеет просто уйму функций.

E-mail. Этот вид троянов работает по принципу отправки информации хозяину на e-mail. Следует сказать, что на e-mail пересылают пароли практически на все, что есть на компьютере: Dial-Up, ICQ, e-mail. А некоторые трояны высылают даже номера телефонов

3. **Хакерство и безопасность в сети**.

провайдера, настройку DNS и т.д. Одним словом, этот вид просто занимается сбором информации, и жертва злоумышленника даже может не знать, что ее пароли уже давно кому-то известны, иногда жертва об этом догадывается только тогда, когда приходит счет от провайдера. Этот вид в основном состоит из 2-х файлов: сам троян и файл для его конфигурирования.

Key Logger. Принцип прост: записывает все клавиши в отдельный файл и затем он, как и e-mail троян, высылает этот файл к хозяину на e-mail. На мой взгляд, он самый примитивный, но хорош в использовании когда жертва при соединении с интернетом не ставит галочку "Запомнить мой пароль".

Pinch - утилита для создания всех видов троянов от загрузчиков до воров паролей. PandaLabs обнаружила Pinch - утилиту для создания троянов, которая продается на нескольких онлайновых форумах. Утилита позволяет кибер-преступникам наделять созданные трояны целым рядом вредоносных функций. “Основная опасность Pinch заключается в том, что утилита очень проста в использовании, поэтому любой начинающий злоумышленник с базовыми знаниями компьютера может очень быстро создать своего трояна, потратив на это совсем немного денег”, объясняет Луис Корронс, технический директор PandaLabs.

4. **Сёрфинг в сети**

Что такоё серфинг и зачем он нужен.



Слово сёрфинг в терминах интернета, появился не так уж и давно. Просматривая сайты один за одним, вы уже являетесь «сёрфером», так же как и серфингисты плывут по волнам, так и вы плывёте на просторах интернета от сайта к сайту в поиске нужной для вас информации. Часто этот термин встречается на сайтах о заработке. Такие сайты предлагают вам зарегистрироваться и работать на них. То есть ваша задача заключается в том, чтобы вы открывали предложенные вам ссылки, ждали некоторое время (обычно 30 секунд), закрывали окно, и переходили к новой ссылке. За каждый просмотр предлагают от 0.01 до 0.1 цента. Смысл такого бизнеса со стороны ваших работодателей, заключается в том, что, к примеру, у меня есть сайт, и я хочу, чтобы люди его посещали, тогда мой сайт будет популярным, и счётчики подсчётов пришедших на сайт посетителей вырастут. Этого я и хочу добиться. Я иду на сайт для сёрфинга, и выкладываю, какую-то сумму денег, и свою ссылку. Каждый день, вы и такие же пользователи как вы, идут по моей ссылке, сидят там 30 секунд, и уходят. Мои счётчики растут. Теперь я могу делать со своего сайта деньги за рекламу. А вы сделали свои деньги, копейки конечно, но все, же деньги. На таком бизнесе вы много не заработаете, но сайты, предоставляющие вам ссылки,

4. **Сёрфинг в сети**

зарабатывают с таких как я немало денег. Выигрываю, конечно, и я, и они. Вы как бы остаётесь в проигрыше. Примерных ссылок на такие сайты давать не хочу, дабы не делать тут рекламу. Поэтому если вы заинтересовались, вы всегда можете выйти в поиск и найти такие сайты.

Как обезопасить свой сёрфинг.

Предлагаем вашему вниманию версию по Настройке безопасности браузера для серфинга сети, от сайта WebMoney.

На современном этапе развития браузерных технологий можно без труда настроить браузер таким образом, чтобы осуществлять безопасный серфинг, не опасаясь за сохранность средств или информации на компьютере. В изложенной ниже инструкции пойдет речь о настройке браузера Microsoft Internet Explorer версии 6.0 и выше. При использовании такого же браузера версии ниже чем 6.0 настоятельно рекомендуется обновить версию браузера до 6.0 и выше. При использовании браузера другой фирмы производителя (Netscape Navigator, Opera и др.), можно предположить наличие у пользователя продвинутого уровня, и возможности без труда разобраться в защите браузера самостоятельно.

Автоматическая настройка параметров Internet Explorer **в режиме сильной защиты**:

- *Настройка общих параметров безопасности браузера: проверка аннулирования сертификатов серверов, разрешение протоколов SSL, проверка аннулирования сертификатов издателей, проверка подписи для загружаемых программ.*
- *Добавление сайтов и сервисов системы WebMoney Transfer в зону "Надежные узлы".*
- *Настройка безопасности зоны "Надежные узлы": разрешение загрузки и использования подписанных элементов ActiveX, разрешение выполнения активных сценариев (скриптов), разрешение выполнения сценариев приложений Java.*
- *Перевод браузера на максимально защищенный уровень для зоны "Интернет".*

Автоматическая настройка параметров Internet Explorer **в пользовательском режиме защиты**:

- *Настройка общих параметров безопасности браузера: проверка аннулирования сертификатов серверов, разрешение протоколов SSL, проверка аннулирования сертификатов издателей, проверка подписи для загружаемых программ.*
- *Добавление сайтов и сервисов системы WebMoney Transfe rв зону "Надежные узлы".*

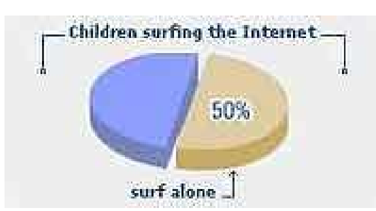
4. **Сёрфинг в сети**

- *Настройка безопасности зоны "Надежные узлы": разрешение загрузки и использования подписанных элементов ActiveX, разрешение выполнения активных сценариев (скриптов), разрешение выполнения сценариев приложений Java.*
- *Настройки браузера для зоны "Интернет" остаются пользовательские.*

Данные утилиты, и более подробную информацию вы можете найти на сайте WebMoney.

Мой ребёнок в сети интернет.

Уже давно для многих Интернет стал жизненно необходимой вещью, без которой Homo Sapiens уже не Homo Sapiens. Было бы достаточно банально перечислять все блага вездесущего потомка Arpanet, тем не менее, факт остается фактом — мы глубоко «погрязли» в паутине и отказаться от этого изобретения человечества многим просто не под силу, особенно если эти многие — дети. Специфика человеческой психики такова, что мы быстро привыкаем к новой среде, в которой комфортно себя чувствуем, изоляция же нас из этой среды равносильна насилию.



Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Согласно последней статистике (сайт) около **50%** детей выходят в Сеть без контроля взрослых:

28% из вышедших в Интернет детей «серфят» в поисках «клубнички»:



По данным вышеупомянутого исследования, **19%** детей иногда посещают порносайты, еще **9%** делают это регулярно. **38%** детей, просматривают страницы о насилии, **16%** детей просматривают страницы с расистским содержимым, **26%** детей участвуют в чатах о сексе.

4. **Сёрфинг в сети**

Продолжая статистику:

25% пятилетних детей активно используют Интернет. Уже в **2001** году **25%** пятилетних детей в США пользовались Интернетом. Эта цифра достигает **75%** среди детей возраста **15–17** лет. Данные, собранные в результате опроса «Использование компьютера и Интернета детьми и подростками в **2001** году», проведенного департаментом образования США показывают, что дети начинают пользоваться Интернетом в самом раннем возрасте.

В **2004** году Интернетом пользовалось больше детей, чем взрослых. Дети опережают взрослых по количеству времени, которое они проводят в Интернете. Это одно из заключений Ассоциации исследования средств коммуникации **(Association for the Research of Communication Media)** после проведенного в **2004** году опроса пользователей Интернета. Конкретные данные указывают на то, что только в возрасте между **8** и **13** годами дети составляют половину общего числа пользователей Интернета. Большинство из них выходит в Сеть из дома и самыми частыми их занятиями являются браузинг, чаты и онлайновые игры.

44% детей подвергались сексуальным домогательствам в Интернете. По данным исследования, опубликованного в **2002** году в Испании Агентством Защиты Детей **(Child Protection Agency)**, **44%** детей, регулярно использующих Интернет, один раз подвергались сексуальным домогательствам при виртуальном общении, **11%** подверглись им несколько раз. В других случаях, воздействие может принимать форму оскорблений со стороны других интернет–пользователей или почтовых сообщений с оскорбительным содержанием. Тревожные данные: **14.5%** детей, принявших участие в опросе, назначали встречи с незнакомцами через Интернет, **10%** из них ходили на встречи в одиночку, а **7%** никому не сообщили, что с кем–то встречаются.

Как воспитывать своего ребенка в контексте интернет–безопасности — дело каждого, иногда достаточно просто строгого слова родителя. Тем не менее, сам факт существования руководств, содержание одного из которых приведено ниже, говорит об актуальности темы и ее крайней значимости. Нижеследующий «мануал» не претендует на звание полноценной всеобъемлющей инструкции и представлен как один из примеров авторитетного руководства представительства корпорации **Microsoft** в России. Возможно, многим читателям руководство покажется

немного наивным — однако не будем забывать во сколько лет современные дети выходят в Сеть;)

Microsoft советует…
Десять фактов, которые нужно сообщить детям ради безопасности в Интернете

Интернет может быть прекрасным местом как для обучения, так и для отдыха и общения с друзьями. Но как и весь реальный мир, Сеть тоже может быть опасна. Перед тем как разрешить детям выходить в Интернет самостоятельно, следует установить ряд правил, **с** которыми должен согласиться ваш ребенок.
Если вы не уверены, с чего начать, вот несколько рекомендаций, как сделать посещение Интернета для детей полностью безопасным.

1. Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми.
2. Научите детей доверять интуиции. Если их в Интернете что–либо беспокоит, им следует сообщить об этом вам.
3. Если дети общаются в чатах, используют программы мгновенного обмена сообщениями, или занимаются чем–то иным, требующим регистрационного имени, помогите ребенку его выбрать и убедитесь, что оно не содержит никакой личной информации.

4. Настаивайте на том, чтобы дети никогда не выдавали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки.
5. Объясните детям, что разница между правильным и неправильным одинакова: как в и Интернете, так и в реальной жизни.
6. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.
7. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование чужой работы — музыки, компьютерных игр и других программ — является кражей.
8. Скажите детям, что им никогда не следует встречаться с друзьями из Интернета. Объясните, что эти люди могут оказаться совсем не теми, за кого себя выдают.
9. Скажите детям, что не все, что они читают или видят в Интернете, — правда. Приучите их спрашивать вас, если они не уверены.
10. Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное

содержимое, выяснить, какие сайты посещает ребенок и что он делает на них.

Горячий FAQ

В каком возрасте следует разрешить детям посещение Интернета?

Дети начинают пользоваться Интернетом во все более и более раннем возрасте. Дети уже в возрасте семи лет могут пользоваться Интернетом в школе, поэтому, скорее всего, захотят иметь в доступ в Сеть и дома. Однако у тех, кто еще не достиг десятилетнего возраста, обычно нет навыков критического мышления, столь необходимого для самостоятельного посещения Интернета. Поэтому всякий раз, когда дети выходят в Сеть, садитесь рядом и следите за тем, чтобы они посещали только те сайты, которые выбрали вы. Внушите им, что никогда нельзя сообщать в Интернете личные сведения.

Следует ли разрешать детям иметь собственные учетные записи электронной почты?

Предпочтительнее, чтобы дети пользовались общим семейным адресом, а не собственным ящиком. Когда они станут старше и будут настаивать на своей независимости, тогда можно будет завести для них отдельный адрес. Однако корреспонденция может по–прежнему оставаться в семейном почтовом ящике. Это позволит родителям держать под контролем все сообщения, адресованные ребенку.

Какими внутрисемейными правилами следует руководствоваться при использовании Интернета?

Выработайте вместе с детьми соглашение по использованию Интернета. В нем должны быть описаны права и обязанности для каждого члена семьи. А также — четко сформулированы следующие пункты.

4. **Сёрфинг в сети**

. Какие сайты могут посещать дети и что им разрешается там делать.
. Сколько времени ваши дети могут проводить в Интернете.
. Что делать, если что–нибудь вызывает у ваших детей ощущение дискомфорта.
. Как защитить личные данные.
. Как следить за безопасностью.
. Как вести себя вежливо и корректно.
. Как пользоваться службами чатов, группами новостей и мгновенными сообщениями.

Для эффективности такого соглашения крайне важно участие детей в его составлении. Распечатайте его и держите рядом с компьютером для напоминания всем членам семьи, регулярно просматривайте и вносите изменения по мере того, как дети взрослеют.

Как дети могут обезопасить себя при пользовании службами мгновенных сообщений?

Помогите детям освоить принципы безопасности. Вот некоторые рекомендации по правилам использования служб мгновенных сообщений (например, **MSN Messenger**):
. Никогда не заполняйте графу «личные данные» или профиль в каталоге пользователей (их может просмотреть каждый).
. Никогда не разговаривайте в Интернете с теми, чей адрес электронной почты или имя вам незнакомы. Родители должны регулярно проверять список контактов своих детей, чтобы удостовериться, что они знают всех, с кем общаются их дети.
. Внимательно просматривайте новые запросы на включение в список друзей. Если вы не хотите добавлять кого–то в этот список, этого человека можно всегда заблокировать.
. Никогда не используйте систему мгновенных сообщений для распространения слухов, сплетен или злобных сообщений.
Открытый и доброжелательный диалог с детьми гораздо конструктивнее, чем тайная слежка за ними. В вопросах технологии они всегда будут на шаг впереди вас. Вам лишь необходимо разработать хорошие правила, верить в то, что дети будут их выполнять и с течением времени вносить в них изменения.

4. **Сёрфинг в сети**

Могут ли дети стать интернет–зависимыми?

Интернет — замечательный инструмент для молодежи; особенно для тех, кто испытывает трудности в общении с ровесниками. Дети, которые легко осваивают компьютер, могут выделиться на фоне других в Интернете, потому что ни внешность, ни физические данные здесь не имеют никакого значения и подростки легко повысят свою самооценку. Однако чрезмерное использование компьютера может привести к еще большей изоляции застенчивых детей. Или отвлечь от других важных занятий, таких как домашние задания, спорт, сон или общение со сверстниками. Родители и учителя часто не осознают этой проблемы до тех пор, пока она не становится очень серьезной. Это связано с тем, что легко скрыть многочасовое сидение в Интернете. К тому же, факт наличия такой болезни как интернет–зависимость, не является широко признанным. Установите правила использования домашнего компьютера и постарайтесь достичь разумного баланса между нахождением в Интернете и физической нагрузкой подростка. Добейтесь, чтобы компьютер находился в общей комнате, а не в комнате

ребенка. В конце концов, спросите себя: не провожу ли я сам в Интернете часы напролет? Если да, то ребенок, скорее всего, следует вашему примеру.

Что должны знать дети о компьютерных вирусах?

Вирус — это вредоносная программа, которая заражает файлы, а затем производит собственные копии. Чем бы ни занимались дети в Интернете, сделать компьютер уязвимым для вирусов можно почти всегда. Самое популярное средство распространения вирусов — электронная почта, а также программы для обмена файлами и системы мгновенных сообщений.

Убедитесь в том, что ваши дети осознают следующее:
. Никогда нельзя открывать вложение электронного сообщения, присланного с незнакомого адреса.
. Нужно настроить программу обмена мгновенными сообщениями так, чтобы стало невозможным получать файлы от посторонних людей.
. При использовании программ обмена никогда не скачивайте файлы, имена которых заканчиваются на **.exe.**
. Перед тем, как скачать какую бы то ни было программу, необходимо

4. **Сёрфинг в сети**

чтобы ее проверили родители.
Для надежной защиты компьютера нужно всегда запускать обновленные версии брандмауэра и антивирусного обеспечения, а также периодически проверять компьютер на наличие шпионов или других нежелательных программ и немедленно удалять их.

Меня беспокоит то, что мои дети пользуются Интернетом. Могу ли я проследить, какие места они посещают?

Да, есть способы, позволяющие проследить, в каких местах Интернета они побывали. Однако имейте в виду, что дети, которые с компьютером на «ты», знают как замести свои следы. Гораздо более эффективный способ — создание четких правил по использованию Интернета и откровенное общение с детьми. Когда вы перемещаетесь по Интернету, браузер собирает всю информацию о посещенных местах и сохраняет ее на компьютере. Современные браузеры обычно ведут журнал последних посещенных сайтов.
Обозреватели создают также временные копии страниц, известные как кэш–файлы. Для просмотра временных файлов с помощью обозревателя **Internet Explorer**:
1.Находясь в **Internet Explorer**, щелкните на Сервис, затем выберите «Свойства обозревателя».
2.На вкладке «Общие», в зоне «Временные файлы Интернета», щелкните на кнопку «Настройка».
3.В зоне «Папка временных файлов Интернета» щелкните на кнопку «Просмотреть файлы».
4.Просмотрите список сайтов, которые недавно посещали вы и ваш ребенок, а также изображения и **cookie**–файлы.

Что следует предпринять, если моего ребенка преследуют в Интернете?

Такие действия часто называют грифингом или попросту хулиганством — очень распространенное явление. Если началось преследование, «нехорошего» человека можно попросту заблокировать. Сохраните все электронные письма, исходящие от преследователя и перешлите их своему провайдеру для принятия соответствующих мер.

4. **Сёрфинг в сети**

Помогает ли фильтрующее программное обеспечение?

Средства фильтрации хорошо дополняют, но не заменяют, контроль родителей за маленькими детьми. К тому же, эти программы зачастую попросту не справляются с отсеиванием нежелательного материала. Они могут блокировать действительно полезную информацию, нужную, например, вашим детям для выполнения домашнего задания. Все–таки, по мере их взросления необходимо развивать навыки безопасного и ответственного поведения в Интернете.

Мой сын–подросток хочет делать покупки в Интернете. Как можно убедиться в надежности сайта?

Перед тем, как разрешить использование вашей кредитной карточки в Интернете, вы должны дать четкие инструкции: как приобретать товар и как убедиться, что процесс покупки надежный и безопасный. Перед тем, как покупать что–то на сайте, поищите:
. значок с изображением закрытого замка в нижнем углу страницы — он указывает на то, что о финансовой операции будете знать только вы и система поддержки сайта;
. строчку **https (s** означает «защищено») в адресе.
Но, к сожалению, все это можно подделать. Поэтому убедите детей сначала советоваться с вами перед тем, как что покупать в онлайне. Убедитесь в том, что ваш браузер поддерживает **128**–битное шифрование — в таком случае номер вашей кредитной карты автоматически шифруется перед отправкой. На какие положения политики конфиденциальности детского сайта нужно обращать внимание**?** В политике конфиденциальности сайта описываются варианты использования, распространения и хранения личных данных, собираемых сервером. Очень важно, чтобы родители внимательно прочитали все положения сайта и показали детям, на что следует обратить особое внимание. Иногда эти положения могут оказаться длинными, запутанными и неопределенными. Если у сайта нет политики конфиденциальности или какой бы то ни было декларации — соблюдайте осторожность, делая покупки или предоставляя личные данные этом серверу.

Следует обращать внимание на:
. тип информации, собираемой и отслеживаемой сайтом;
. способ использования полученных данных (особенно тот пункт, где

может быть указана возможность продажи информации третьей стороне); . возможность удаления или внесения изменений в данные, полученные от вашего ребенка;
. какие шаги предпринимаются для охраны детей в чате, а также при использовании ими досок объявлений и электронной почты;
. стремится ли сайт получить согласие родителей, прежде чем ребенок сообщит свои личные данные.

Логин и пароль, а так же надоевшая captcha.

Логин [Login] – это имя пользователя. От пароля отличается тем, что логин не секретный, от имени – тем, что не общедоступный. Логин нужен системе для идентификации пользователя: чтобы войти, например, на форум, требуется ввести логин в специальную строку и подтвердить паролем. Таким образом, система опознает и впускает пользователя.

Пароль [Password] – Секретная комбинация символов или слово, предъявляемые пользователем для получения доступа в автоматизированную систему. Служит для защиты программ и данных от несанкционированного доступа.

Captcha – это аббревиатура от слов «Completely Automatic Public Turing Test to Tell Computers and Humans Apart». В переводе с английского: «полностью автоматизированный публичный текст Тьюринга для различения компьютеров и людей». Нашими словами Каптча – это система позволяющая сайту проверить наличие неискусственного интеллекта. При регистрации на сайте вы можете столкнуться с такими картинками и просьбой ввести в строку то, что написано на такой картинке. Ниже приведены примеры captcha.

redsous	**Google ***** Нелинейное искажение надписи, смещение символов друг относительно друга, близкое расположение символов, различные шрифты. Шумы не применяются. Правда, символы не всегда склеиваются без промежутков.
	MSN **** Поворот и искажения символов, шумы в виде линий того же цвета, пересекающих символы.
	Yahoo *** Нелинейное искажение символов, шум в виде пересекающей символы ломаной.

4. **Сёрфинг в сети**

Смысл такой проверки в том, что человек, который регистрируется, всегда сможет ввести увиденное на картинке, и продолжить регистрацию. Но программа робот, так не умеет, она не видит те буквы и цифры что изображены на картинке. Таким образом, сайт закрывает доступ автоматической регистрации от программ – роботов.

Теперь давайте вернёмся к логину и паролю.

У каждого пользователя, есть свой логин, и пароль для доступа к тому, или другому сайту. Выбор логина, не такое уж и простое дело. Логин, должен иметь, какой ни - будь смысл, который бы описывал вас, как личность, или что то, из вашей жизни. Логин должен быть уникальным, и не повторялся, иначе вас могут спутать с другим пользователем. На форумах, часто бывают кучи разных логинов, и ваш должен выделяться из всех. Логин вида: Alex, Andrey, Marina, Wolf, и т.д., не очень запоминающийся, так как у половины интернета есть такие логины. Все хотят быть Волками, или просто написать на английском своё имя. Если у вас есть фантазия, включайте её, и постарайтесь выбрать самый подходящий для вас логин.

Пароль, всегда при авторизации, регистрации, мы сталкиваемся с вводом пароля. Но стоит ли вообще задумываться о том, какой пароль регистрировать, будет ли он иметь только числа, только буквы, или и числа и буквы вместе. Важно ли то, сколько символов вы ввели в пароль? Ответ один. Да. Всё это очень важно. Самым надёжным паролем являются буквы и цифры, разбросанные в бессмысленном порядке, и такой пароль должен превышать 8 символов. Если вы регистрируетесь на сайте, который вам не очень нужен, вы регистрируетесь, дабы получить ссылку на скачивание, или ещё для чего-то одноразового, ненужно стараться вписать ваш настоящий пароль. Я приведу пример из своего опыта. Я регистрируюсь на сайтах и форумах, где даже если мой account взломают, то я не буду особо горевать. Для таких сайтов и форумов я ставлю пароль, к примеру - 555555. Если же я регистрируюсь, на каком ни будь важном сайте, я ставлю пароль более замысловатый, но недлинный. Если же где то, где мне не как нельзя чтобы меня взломали, я ставлю пароль более длинный и более сложный. Напоминаю, что ставить пароль с датой рождения, тоже не очень умно. Если же вы на каждом сайте ставите галочку сохранить пароль, и даёте браузеру запомнить ваш пароль, знайте, что если вы получите «Троян», вы потеряете все ваши пароли в миг. Почта, клиент для обмена сообщениями, и прочее. Так как такие программы, смотрят на сохраненные пароли в базе браузеров и других программ. Старайтесь каждый раз вписывать пароли, а не сохранять их. Предлагаю вам, посетить сайт, который расскажет вам немного о видах пароля, и о Генераторе пароля. **Посетить сайт**

4. **Сёрфинг в сети**

Взлом паролей.

Взлом паролей — ресурсоёмкая задача, обычно решаемая так называемым методом грубой силы (англ. Brute force) — то есть простым перебором.

Более эффективными в большинстве случаев является перебор по словарю или социальный метод.

По утверждению Брюса Шнайера, наиболее часто используемый пароль — «password1».

Существуют специальные программы для подбора пароля, например: L0phtCrack, John the Ripper, Cain и PasswordsPro.

Также пароли получают, засылая вирус (троян), который локально на чужом компьютере расшифровывает пароли, и скрыто отсылает их создателю вируса.

5. **Почта, интернет пейджеры, электронная коммерция.**

Зачем нужна почта, и как её создать.

Электронная почта, [“и-мэйл”, Email] — система пересылки почтовых сообщений между абонентами, одна из важнейших возможностей Интернета; также называют и сами сообщения, пересылаемые между пользователями. Пользователь имеет закрепленное за ним дисковое пространство на сервере провайдера — почтовый ящик. Благодаря уникальному адресу вся получаемая и отправляемая почта персонифицирована. Почтовая программа предоставляет сведения об отправителе, регистрирует время получения сообщения, обеспечивает сортировку большого объема почты. По каналам электронной почты передаются, в частности, биржевые сводки, платежные документы и совершаются сделки.

Термины, связанные с электронной почтой:

• **Mailbox — "**Почтовый ящик**":** в системах электронной почты**:** файл или каталог**,** куда помещаются пришедшие сообщения**,** предназначенные для конкретного пользователя**.**

• **Gmail* —** популярный почтовый сервис**,** организованный фирмой **Google.** Его характеристики**:** размеры почтовых ящиков **—** до **1** Гбайта**;** предоставляется возможность прикрепления к письму неограниченного количества файлов размером до **10** Мбайт**;** обеспечивается полнотекстовый поиск**,** позволяющий быстро находить любую информацию среди своей почтовой корреспонденции**;** стабильность работы**,** а также возможность автоматического перенаправления почты**;** имеются **SPAM-**фильтры**,** гибкая система фильтрации почты и др**.**

• **Fax-mailbox — "**Факсимильный почтовый ящик**":** аналог почтового ящика электронной почты для факсимильных сообщений**.** Получатель может извлечь из него сообщения в дистанционном режиме**,** набрав соответствующий номер на своем факсимильном аппарате**.**

• **Mailer — "**Почтальон**":** программа**,** обеспечивающая работу электронной почты**.**

• **Mailing list* —** список или подсистема рассылки сообщений**.**

5. **Почта, интернет пейджеры, электронная коммерция.**

• Псевдоним **[alias, nickname] —** простая одноязычная фраза или слово, заменяющие собой в системах электронной почты более длинный адрес, например **<FelixSV>** вместо **<fsv@gpntb.ru>**

• Спам **[Spam, junk mail] —** навязанное адресату электронной почты или пользователю других телекоммуникационных средств и сервисов (например **ICQ, IM,** мобильной связи, телеконференций и др.) сообщение, имеющее рекламно-агитационный характер (в том числе и противозаконный) и часто пересылаемое по большому списку. Спамом также называют все другие виды сообщений не представляющих интереса для абонента. Часто спам отправляется анонимно с подложным адресом отправителя и содержит вирусы.

• Мыло — называют обычную почту. Родилось от слова **mail.** Часто используется глагол: Мылить, намылить, промылить.

Как же создать себе почтовый ящик **(MailBox).** Я, как человек который прошел немало постовых систем таких как:

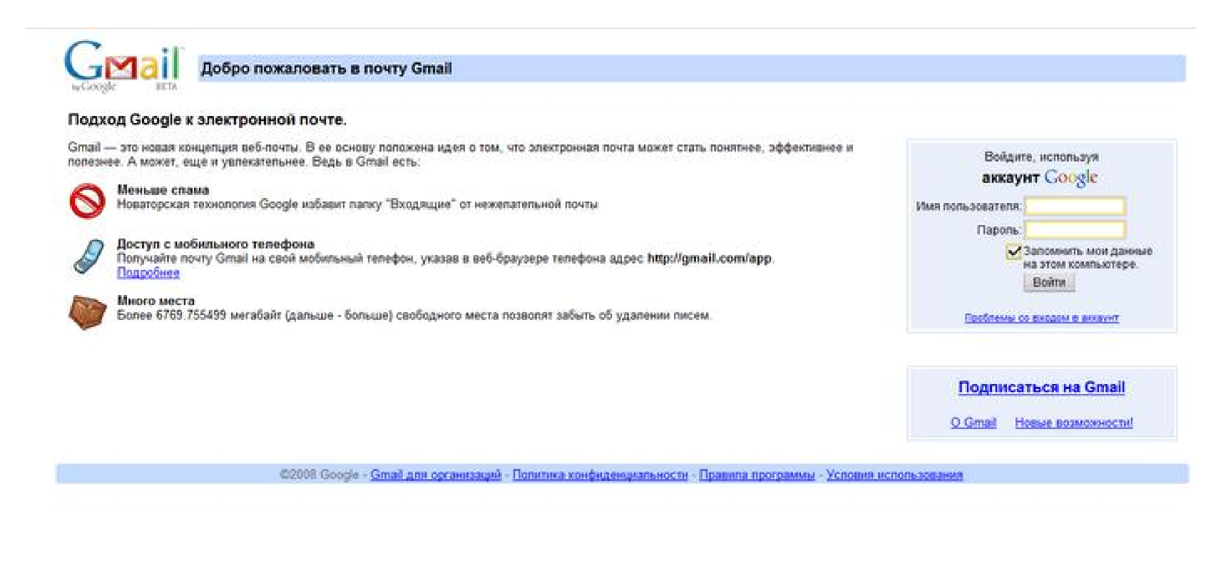
Rambler.ru, Mail.ru, Yandex.ru, Pochta.ru, Xakep.ru, Yahoo.ru, Walla.co.il, Hotmail.com.

Опробовав многие из них, я не был очень довольным. На почтовый ящик **rambler,** мне приходили письма спустя **2** недели, или не приходили вообще. На почту **mail.ru,** всегда приходил, какой-то спам, или куча ненужной мне информации. Так же удобства там ожидают желать лучшего. Максимальная отправка файлов – **10** мегабайт. Все описывать не буду, выбирать вам. Но для себя я выбрал самую лучшую почтовую систему. Я с ней уже не первый год, и очень рад тем чем пользуюсь. Предлагаю вам использовать **Gmail.com**

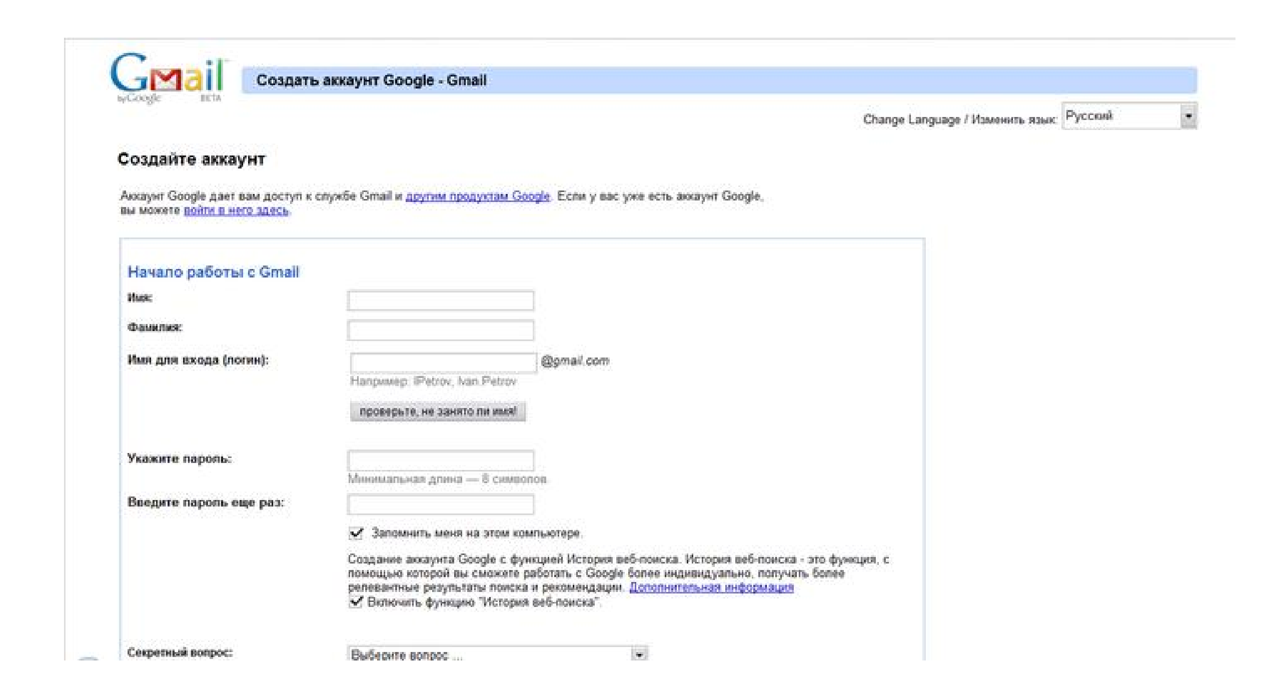
Ниже смотрите пару скриншотов.

5. **Почта, интернет пейджеры, электронная коммерция.**

Главная страница.

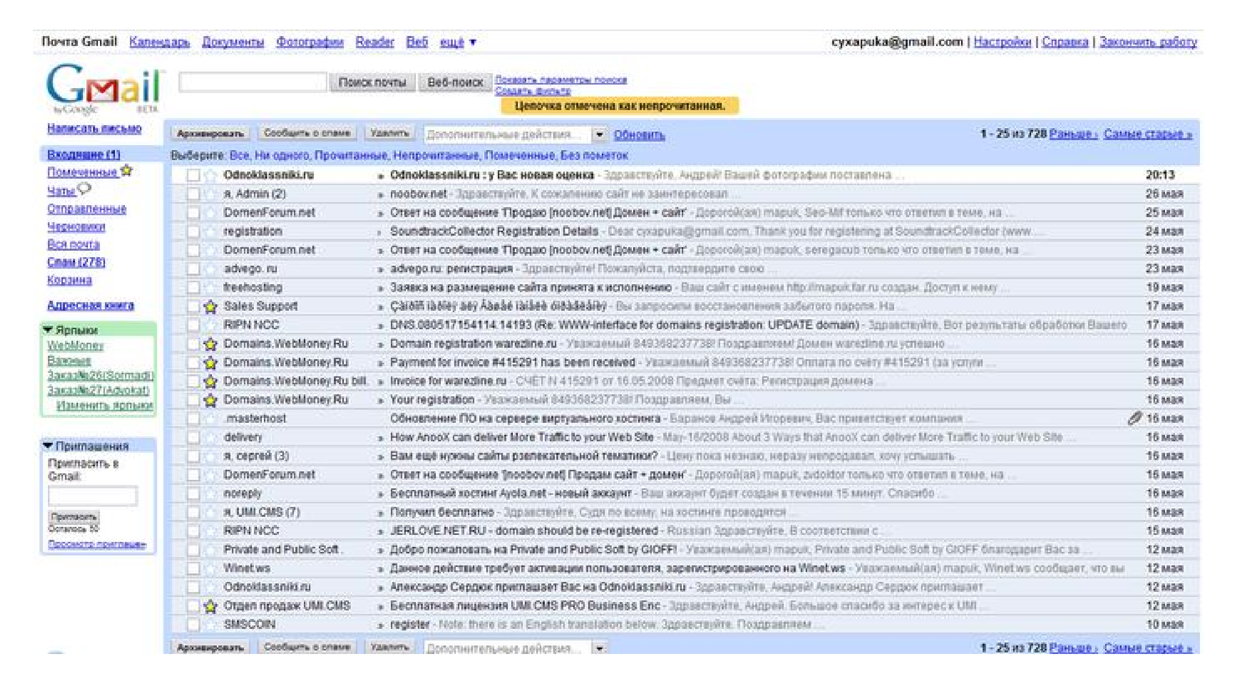


Страница регистрации.



5. **Почта, интернет пейджеры, электронная коммерция.**

Страница просмотра входящих сообщений



[Зарегистрироваться в системе Gmail.com]

Что такое электронная коммерция.

Электронная коммерция - бизнес, основанный на информационных технологиях. Электронная коммерция предполагает:

- открытие своего сайта и виртуального магазина в Интернете;

- наличие системы управления компанией;

- использование электронной рекламы и маркетинга;

- использование моделей бизнес для бизнеса и/или бизнес для потребителя.

Оплата в таком бизнесе производиться посредствам интернет кошельков различных систем. Самая популярная русская система оплаты, через интернет, является webmoney.

Так же в Ру.Нете существуют такие системы как **Яндекс.Деньги**, RuPay, и ещё некоторые менее известные, но всё же активные. Во всём мире всем известны системы PayPal, E-Gold. Так же часто на сайтах предлагают расплатиться карточкой Visa, или MasterCard, что является самым опасным методом покупки товаров через интернет. Сильно углубляться я

5. Почта, интернет пейджеры, электронная коммерция.

не буду в мир интернет коммерции, кто как зарабатывает, и что продаёт. Но хочу немного рассказать о «кардерах»

Кардинг - это существенная угроза е-коммерциии вообще и е-банкингу в частности.

Кардинг – это незаконное использование кредитных карт для покупки различных товаров и услуг.

Кардер - соответственно человек, который использует ворованные кредитные карточки.

Как правила работает это так.

Кардером или группой кардеров организуется сайт, чащё всего это порно-сайт, и чтобы пользователи могли получить доступ к клубничке необходимо заплатить небольшую сумму денег, порядка 5$/год. Естественно вы расплачиваетесь по кредитной карте, и в этом случае могу вас заверить, как только вы это сделаете её номер оказываться в руках преступников.

Самым же распространенным способом получения номеров кредитных карт является взлом легальных и работающих интернет - магазинов. Дело в том, что интернет магазины это такое же программное обеспечение скажем как ваш Windows, а как следствие оно также содержит ошибки. Для примера приведу следующую историю : недавно одним из хакеров была обнаружена ошибка в очень распространенном ПО для интернет - магазинов cart32. Следствием умелой обработки хакерами этой ошибки стало получения доступа к базе содержащей номера кредитных карт клиентов этого интернет - магазина. Конечно, весть про эту ошибку с огромной скоростью распространилась в среде кардеров и хакеров, и как следствие по этому шаблону было взломано ещё несколько десятков магазинов по всему миру, но к счастью остальные магазины скачали и установили программу-заплатку устраняющую ошибку. Но где гарантия, что сегодня - завтра не найдется новой ошибки?

Главный вывод - по возможности делайте покупки в крупных магазинах. И не смотря на то, что сведения о взломе того или иного интернет - магазина приходят тоже довольно часто, но всё же на крупных сайтах более основательно подходят к вопросам безопасности. Все серьёзные интернет - магазины, во-первых, использую очень надёжное ПО, например, в качестве ОС там используется ОС FreeBSD. В сумме с грамотной настройкой и постоянным администрированием – это составляет почти непреодолимую преграду для хакеров. Также там собственно используеться более дорогое и более качественное ПО интернет-магазина, вовремя с сайта разработчика скачиваються заплатки и дополнения.

5. **Почта, интернет пейджеры, электронная коммерция.**

Мой web пейджер

ICQ – Практически исходник для остальных подражателей. Все стандартные функции (чат, видео/аудио, передача файлов, хистори, смайлы...) очень удобная функция невидимки и возможность оперирования с контакт-листом (группирование, визибл/инвизибл листы, бан). Наверное один из самых популярных мессенджеров, если и вовсе не самый популярный. Сам не пользуюсь давно, но по крайней мере раньше никакой стыковки с другими ИМ не было.



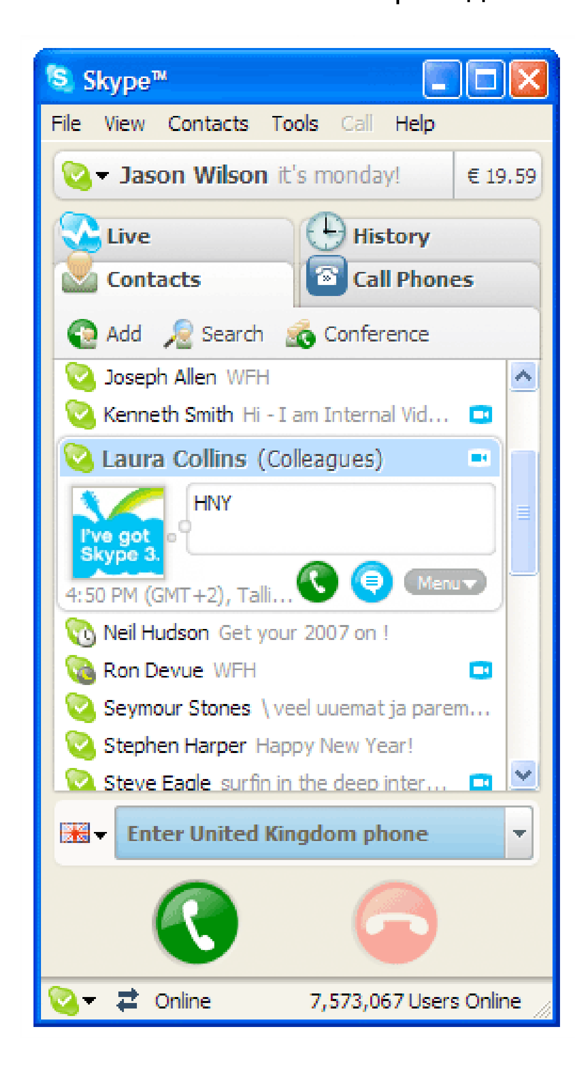
5. **Почта, интернет пейджеры, электронная коммерция.**

MSN - наверное так же в представлении не нуждается. Интеграции с другими пэйджерами нет. Скины можно менять лишь путем смены фона. Визуально приятный интерфейс. Скринмэйты, смайлы, аудио/видео, игры, связан с мылом по которому вы получаете аккаунт – то есть действует заодно и как чеккер мыла. Еще множество приятных мелочей, типа смена комментария вашего Ника в зависимости от песни проигрываемой в виндоузмедиа плеере. Смело могу сказать, что комп негрузит, по крайней мере относительно.



5. **Почта, интернет пейджеры, электронная коммерция.**

Skype - Это простая бесплатная программа, с помощью которой вы можете звонить во все уголки мира. Сеть **Skype** базируется на прогрессивной **P2P (peer-to-peer)** технологии. Качество передачи голоса очень хорошее. **Skype** предоставляет максимальную конфиденциальность - все общение между клиентами зашифровано и не может быть перехвачено. Кроме этого программа позволяет общаться с помощью коротких текстовых сообщений. Начиная с версии **2.0** в программе **Skype** появилась возможность проводить видеоконференции.



5. **Почта, интернет пейджеры, электронная коммерция.**

Yahoo Messenger - уведомит вас и поступлении корреспонденции в ваш почтовый ящик **Yahoo Mail** и предупредит вас о приближающейся важной дате, занесенной в **Yahoo Calendar**.

Поддерживает работу с файервол, может быть минимизирован до ярлыка в ожидании Интернет-соединения, предоставляет возможность распечатать диалог собеседников, вести голосовой чат. Среди других возможностей - создание чат-комнат, отправление сообщений респондентам, которые не находятся в текущий момент в режиме **online** и пр.



5. **Почта, интернет пейджеры, электронная коммерция.**

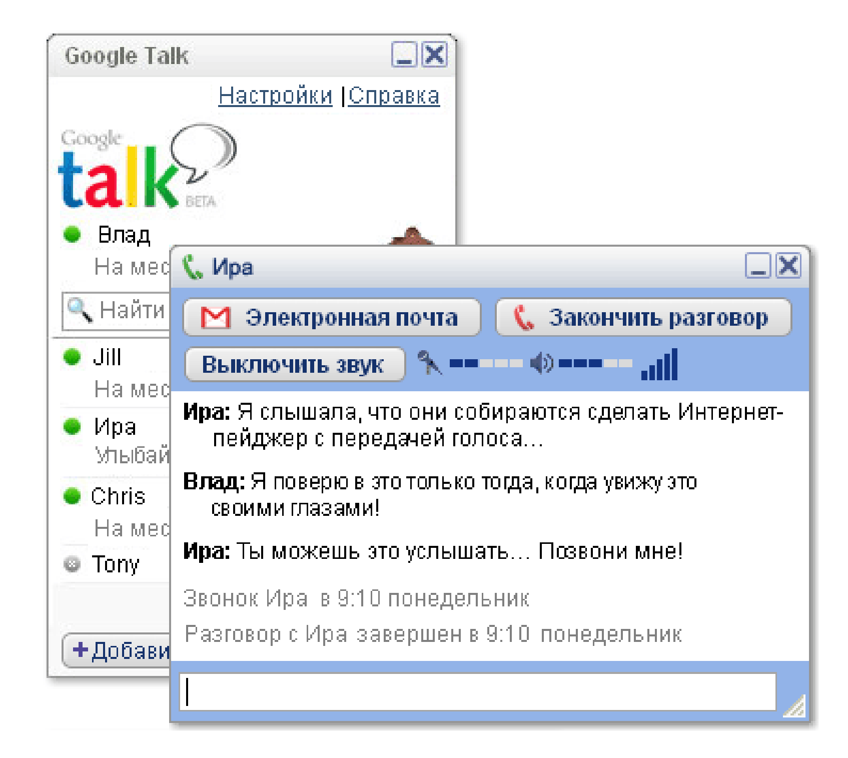
Miranda - небольшой клон **ICQ**, предназначенный для тех, кто использует **ICQ** прежде всего для общения с помощью мгновенных сообщений. Включает в себя многопользовательскую поддержку и прочие полезности, включая чтение сообщений голосом. Плагинов много, начиная с плагина, для проверки почты и заканчивая плагином для изменения стиля отображения сообщений.





5. **Почта, интернет пейджеры, электронная коммерция.**

Google talk- Программа позволяет обмениваться через сеть **Internet** короткими сообщениями и совершать бесплатные звонки**.** Особенность заключается в тесной интеграции с почтовой службой **GMail:** например**, Google Talk** периодически проверяет почтовый ящик и выводит уведомления**.** Обязательное условие использования **Google Talk -** наличие почтового ящика в системе **GMail.**



5. **Почта, интернет пейджеры, электронная коммерция.**

PalTalk - современное средство общения, объединяющее в себе обычный чат, голосовой чат и видео-чат. В отличие от **ICQ**, и подобных программ, **PalTalk** нацелен не только на приватное обещение **Tet-a-Tet**, но и на одновременное общение с большим числом людей в тематических комнатах. При этом все присутствующие могут видеть и слышать друг друга.



5. **Почта, интернет пейджеры, электронная коммерция.**

AIM (AOL) - передача сообщений, файлов, аудио, видео; игры с собеседником. Вроде никаких скинов, никакой интеграции с остальными мессенджерами. Предлагается зарегистрировать и почту на **2** гигабайта.



5. **Почта, интернет пейджеры, электронная коммерция.**



Быстрый и простой способ подключения нескольких интернет-пейджеров в одном месте: **AOL, Yahoo!, ICQ, Jabber, GTalk, MSN** и собственный **MeeboMe service.**

Не требуется установка программного обеспечения. Популярность **Meebo** растет быстрее, чем **Google Talk.**

Есть Многоязыковая поддержка. **Перейти на сайт.**

Как уберечься от взлома

В последнее время одним из видов криминального бизнеса стал взлом электронных почтовых ящиков. Профессиональные хакеры по сдельной цене готовы добыть пароль доступа к данным любых юридических или физических лиц

Секретная информация в наше время стоит дорого. Не важно, кому она принадлежит: крупной фирме или простому обывателю. Жертвой хакерской атаки может стать любой: для того чтобы «набить руку», начинающий взломщик может наугад выбрать «жертву» и уничтожить принадлежащие ей профайлы.

Чтобы защитить свой номер **ICQ** от взлома есть пару довольно эффективных примеров.

1. Использовать безопасные клиенты, что под этим подразумевается?

Безопасный клиент это тот, который не отображает ваш **ip** адрес. Безопасные клиенты это **QIP, Miranda, RQ.**

2. НИКОГДА не сохранять пароль в клиенте! Спросите почему? Если Ваш компьютер будет заражен вирусом, вирус отошлет Ваш пароль злоумышленнику.

5. **Почта, интернет пейджеры, электронная коммерция.**

3. Поставить сложный, но одновременно запоминающийся Вам пароль:

Пример:

Правильно - **5eRt%+8** (цифры, буквы, регистр, знаки) - скорость взлома около **300** лет

Неправильно - **alena17** (слово, цифры) - скорость взлома **10** минут

4. НИ ОТ КОГО не принимать файлы, а лучше вообще отключить эту функцию. Почему?

а) антивирус вас не сможет защитить

б) даже если это знакомый человек его номер может быть угнан и вас он еще не успел предупредить

в) даже если это будет не вирус, злоумышленник узнает ваш **ip** адрес и потом сможет провести атаку на Ваш компьютер

5. Никому не говорите свой пароль.

6. Никогда не меняйте пароль в нетрезвом состоянии (проверено на личном опыте)

7. Выставляйте сложные контрольные вопросы, которые не так просто угадать, но одновременно легко вам запомнить.

8. Если у Вас уже сохранен пароль в клиенте. То необязательно переустанавливать систему, чтобы его стереть, достаточно убрать галочку "сохранить пароль" и поменять пароль.

9. Своевременно обновлять клиент **icq**, так как с выходом обновленной версии клиента меняется способ криптования (шифровки паролей) и троян попросту не сможет расшифровать Ваш пароль.

10. Своевременное а лучше каждодневное обновление антивирусного програмного обеспечения и операционной системы для обнаружения новых троянов и вирусов.

11. Если Вы покупаете номер или Вам его дарят, то лично я бы рекомендовал следующую схему построения инфо, для максимальной защиты от спама:

5. **Почта, интернет пейджеры, электронная коммерция.**

Оптимальная настройка icq

Ник: Ваш ник

Имя: Ваше имя

Домашний адрес: Здесь лучше его не указывать

Компания: ваша компания

Пол: нет смысла если написали имя

Язык: не указывать

Интересы: Если в них что-нибудь указать то по этим интересам и будете получать спам)

О себе: Вот здесь можно написать ваш город и другую нужную информацию.

Что такое «Социальная сеть».

Социальная сеть (англ. **social network**) — социальная структура (математически — граф), состоящая из группы узлов, которыми являются социальные объекты (люди или организации), и связей между ними (социальных взаимоотношений).

Начало современной теории социальных сетей положили в **1951** году Рэй Соломонофф **(Ray Solomonoff)** и Анатолий Рапопорт **(Anatol Rapoport)**. В **1959–1968** гг. венгерские математики Пол Эрдос **(Paul Erdos)** и Альфред Реньи **(Alfred Renyi)** написали восемь статей, описывающих принципы формирования социальных сетей. Дункан Уоттс **(Duncan J. Watts)** и Стивен Строгач **(Steven H. Strogatz)** развили теорию социальных сетей, и в числе многих других открытий ввели понятие коэффициента кластеризации **(clustering coefficient)** – степени близости между неоднородными группами.

5. **Почта, интернет пейджеры, электронная коммерция.**

Влияние индустрии социальных сетей на современную жизнь неоспоримо, и в настоящий момент социальные сети эволюционируют наиболее значительным образом – они движутся к новой категории сетей – Социальным Сетям версии **3.0 (Social Networks 3.0).**

Первые социальные сети появились в середине **90-**х годов и предоставляли пользователям начальные возможности для общения, подобно **eGroups/OneList, ICQ, Evite.** Такие сетевые сервисы как правило не рассматриваются в качестве социальных сетей, но тем не менее они являются тем самым фундаментом, на котором в дальнейшем развивались онлайн-услуги для общения и взаимодействия пользователей.

Социальные сети **2.0** появились в начале **21-**го века, когда предприниматели разобрались в сущности социальных сетей и определились с теми широчайшими возможностями, которые предоставляют социальные сети для всех сфер деятельности. Сервисы подобные **Friendster, Tribe, Orkut, LinkedIn, Spoke** позволили создавать социальные сети для отдыха и для работы. Иными словами, в то время создатели социальных сетей работали скорее ради самих сетей и их развития, нежели ради использования возможностей предоставляемых этими сетями.

Ныне мы вступили в третью эпоху социальных сетей. После эйфории участия ради участия, нынешние сети становятся рабочим инструментом, и, более того, необходимым инструментом для ведения деятельности, будь то бизнес или творчество. Социальные сети служат площадкой для неформального общения приятелей подобно **LiveJournal.** Социальные сети помогают создавать новую музыку как **MySpace.** Социальные сети расширяют игровой опыт массовых онлайн-игр в сети **Xfire.** Социальные сети служат серьезным инструментом для поиска сотрудников и партнеров в **LinkedIn.**

Таким образом, социальные сети являются ключевым элементом для дальнейшего развития сообществ и в скором времени они будут неотъемлемым инструментом для любой деятельности.

5. **Почта, интернет пейджеры, электронная коммерция.**

Социальные сети продолжают победное шествие по Интернету. Несмотря на относительную молодость – социальным сетям как онлайновому интернет-сервису чуть больше десяти лет – они пользуются огромной популярностью. По статистике **comScore**, только за последний год количество их пользователей выросло в несколько раз.

Недавно в Рунете появилась оригинальная социальная сеть на карте, «**МирТесен**». Сеть следующего поколения как сервис выполнена на очень высоком уровне и по праву претендует на звание самой красивой – в этом проекте весьма органично используются карты **Google Maps.** Этот новый проект успешно прошел тестирование, открыт для всех желающих и уже пользуется заслуженной популярностью. Пространственный аспект вносит совершенно новые краски в создание связей между людьми. Все становится наглядней, интересней и практичнее.

Так же очень популярным сайтов в ру.нете стал сайт «**ВКонтакте**»

Считается самым посещаемым сайтом ру.нета. Видео галереи, фотогалереи, друзья, группы. И многое другое.

Спам и война с ним

Для того чтобы эффективно бороться со спамом, необходимо четко определить, что именно подразумевается под словом «спам». Нередко провайдеры и владельцы сетей предпочитают руководствоваться «презумпцией виновности», относя к спаму практически всю почту, которую не запрашивал получатель. За последние полтора года эксперты изучили все существующие виды и категории спама и пришли к выводу, что при огульном отнесении к спаму любого нежелательного или рекламного письма возникает большая опасность потерять деловую почту.

«Бытовые» определения спама как «нежелательной почты» или «незапрошенной рекламной рассылки», которые можно услышать от пользователей, провайдеров или владельцев компьютерных сетей, не выдерживают критики.

5. **Почта, интернет пейджеры, электронная коммерция.**

Поскольку при фильтрации спама главное — не навредить получателю почты, необходимо дать более взвешенное определение.

Вот наиболее точное определение спама: спам — это анонимная массовая незапрошенная рассылка.

Это определение довольно хорошо соотносится с мировой практикой и определениями спама, положенными в основу американского и европейского законодательства о спаме. Кроме того, это определение можно эффективно использовать на практике. Поясним его смысл.

- Анонимная рассылка: мы все страдаем в основном именно от автоматических рассылок, со скрытым или фальсифицированным обратным адресом. В настоящее время не существует спамеров, которые не скрывали бы своего адреса и места рассылки.
- Массовая рассылка: именно массовые рассылки, и только они, являются настоящим бизнесом для спамеров и настоящей проблемой для пользователей. Небольшая рассылка, сделанная по ошибке человеком, не являющимся профессиональным спамером, может быть нежелательной почтой, но не спамом.
- Непрошеная рассылка: очевидно, подписные рассылки и конференции не должны попадать в категорию «спама» (хотя условие анонимности и так в значительной мере это гарантирует).

Важны также и категории, которые мы сознательно не включили в определение спама.

Например, в определение спама часто включают словосочетания «рекламная рассылка» или «коммерческое предложение». На мой взгляд, это неправильно.

Дело в том, что значительная часть спама не преследует рекламных или коммерческих целей. Существуют рассылки политического и агитационного спама, есть также «благотворительные» спамерские письма (призывающие помочь каким-нибудь несчастным). Отдельную категорию составляют мошеннические письма (так называемые нигерийские письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды), а также письма, направленные на кражу паролей и номеров кредитных карт («фишинг»). Еще бывают так называемые «цепочечные письма», то есть письма с просьбой переслать их знакомым («страшилки», «письма счастья»).

5. **Почта, интернет пейджеры, электронная коммерция.**

Есть также вирусные письма, содержащие завлекательный текст и вирусы под видом игрушек, картинок, программ («настоящая история Белоснежки», «С Новым годом!» и т. п.). Все эти письма, как правило, нельзя отнести к рекламе, хотя они являются очевидным спамом.

Спам и целевые коммерческие предложения

Из данного выше определения следует, что коммерческое предложение, явно направленное на адрес получателя и с реальным обратным адресом, — это не спам.

Таким образом, я не считаю спамом непрошеное рекламное письмо, например, приглашение на семинар, посланное лично директору фирмы. Или предложение горнолыжного тура в Шамони с настоящим обратным адресом турфирмы.

Кому-то это может показаться возмутительным, странным и нелогичным, но мы считаем, что делать это различие необходимо — и теоретически, и практически.

Такое письмо также может быть нежелательным и вызывать раздражение. Заметим, что такие письма во многих случаях тоже можно распознать и отфильтровать технически, наряду со спамом. Например, **Kaspersky Anti-Spam** имеет рубрики «Семинары/Конференции», «Туризм» и тому подобные.

Однако прежде чем удалять письма данных категорий, системному администратору стоит согласовать политику обработки спама с отделом маркетинга и **PR**. Вполне возможно, что им нужны подобные письма. Например, коммерческие сотрудники туристических фирм часто с интересом читают туристические предложения и даже спам, а организаторы семинаров и сотрудники кадровых отделов хотели бы получать все приглашения на семинары.

Нежелательная почта

Кроме спама и целевых коммерческих предложений существует еще один вид почтовых сообщений, который часто путают со спамом. Это нежелательная почта. В некоторых случаях незапрошенное и ненужное сообщение спамом не является.

5. **Почта, интернет пейджеры, электронная коммерция.**

Вот некоторые примеры нежелательной почты, которую получатель не заказывал и/или не желает получать:

1. Разного рода ошибки: ошибки автоматических рассыльщиков — технический сбой службы рассылки, запросы на подтверждение подписки на рассылку или какой-то сервис; ошибки людей — например, человек ищет однокурсника, а получатель имеет ту же фамилию и похожий адрес.
2. Разнообразная техническая корреспонденция: сообщения о недоставке письма и других ошибках; автоматические сообщения от антивирусных программ о вирусах в отправленном с вашего адреса письме; экстраординарные или рутинные сообщения от администраторов сервисов (например, о том, что почтовый сервис будет недоступен, или о появлении вируса и пр.). Такие письма для получателя часто выглядят как незапрошенные.
3. Новые возможности общения и бизнеса: деловое письмо от частного лица (фирмы) частному лицу (фирме). Такое письмо часто может служить началом нового контракта, дела, бизнеса. Прямое письмо менеджеру корпорации от рекрутингового агентства — адрес обычно получен неофициально, само письмо справедливо трактуется компанией как угроза бизнесу, в то же время такие письма очень полезны рынку труда и капитала.
4. И, естественно, личные письма от тех, с кем получатель никогда ранее не переписывался: письма от старых знакомых, друзей, агитаторов (например, агитация жителей района против загрязнения парка, и т. п.).

Любое из этих писем является незапрошенным, ибо принимающая сторона его явно не запрашивала. С другой стороны, выбрасывать подобную почту без прочтения нельзя. Из этого следует, что признаки массовости и анонимности являются необходимыми для распознавания тех, кто делает бизнес на спаме.

Политика обращения со спамом и нежелательной почтой

Итак, мы разделяем все незапрошенные сообщения, попавшие в ваш почтовый ящик, на следующие категории:

1. спам, имеющий все признаки анонимной массовой рассылки;
2. целевые коммерческие предложения;
3. нежелательная почта.

5. **Почта, интернет пейджеры, электронная коммерция.**

Спам, несомненно, нужно фильтровать, а затем сохранять в особых папках или помещать в карантин, а иногда сразу удалять — согласно политике компании. Вторую и третью категорию писем также возможно распознавать и фильтровать, но с ними нужно обращаться более осторожно. В компании могут быть разные отделы, которые хотели бы получать различные категории непрошеной почты (администраторам нужны сообщения от сервисов и антивирусов, кадровикам — приглашения на семинары).

Таким образом, системный администратор должен вводить тщательно продуманную политику обработки почты, включающую не только уничтожение спама, но маршрутизацию и хранение незапрошенной и даже нежелательной почты.

Термины и сленг интернета

Термин	Обозначение/Обьяснение
Аккаунт (англ.- account)	Учетная или регистрационная запись. Иногда подразумевается логин в системе.
Доменное имя(адрес) (domain name)	Доменная адресация - упрощенный аналог IP-адреса. Введена для удобства пользователей интернета: легче запомнить тектовое написание адреса, чем числа IP-адреса.
Контент	Информационное наполнение сайта
Корневой каталог(папка)	Как правило- **public.html** корневой каталог для размешения файлов на сервере.
Посетители	Число уникальных посетителей сайта.
Поддомены	Домены **3** уровня.
Размер дискового пространства	Измеряется в мегобайтах(Мв), это общий размер всей информации, хранимой на сервере.
Регистрация домена (имени)	Заявка на закрепление того или иного доменного имени за физическим или юридическим лицом в органицацию имеющую права регистратора или при помощи посредника.
Трафик (traffic)	Может быть исходящим и входящим. это поток информации, проходящей через канал связи, приходящийся на сайт.
Хиты	Общее число просмотров сайта(страниц сайта).
Хосты	Количество просмотров сайта(страниц сайта) только с уникальных IP-адресов.
Хостер (hoster)	Организация, предоставляющая услуги Хостинга, синоним слова Хостинг-провайдер.
Хостинг	Организация, предоставляющая диковое пространствао для размещения сайта.
ASP (Active Server Pages)	Это **Web** страницы содержащие исполняемые сервером скрипты. Используется для создания сложных решений динамических комбинаций **HTML**, скриптов, и компонентов **ActiveX**.
Backup	Резервное копирование всей информации сервера.
C, C++	Часто используемые языки программирования для написания **cgi**-скриптов.

CGI (Common Gateway Interface - интерфейс взаимодействия)	Используется для взаимодействия между **CGI**-скриптами и **Web**-страницами и программами или сценариями. Используется для написания гостевых книг, счетчиков и пр.
CGI-скрипты	Программы для создания динамических **html**-страниц. Наиболее популярные языки для создания **cgi**-скриптов - **Perl, PHP.** Так же используется **C, C++, Visual Basic, AppleScript, Java** и языки командных процессоров **Unix.**
CGI-bin	Директория (папка) на сайте, для размещения **cgi**-скриптов.
Cron	Служба запуска программ сервера по расписанию.
DNS (доменная система имен)	Система обозначений и сопоставлений **IP**-адресов и доменных имен.
E-mail forwarding (E-mail форвадинг)	Автоматическое перенаправление почты, на любые дополнительно заданные адреса.
FTP	Протокол передачи файлов. Используется для доступа и закачки файлов на сервер.
.htaccess	Файл для задания множества полезных настроек. С помощью этого файла Вы можете: запретить доступ к файлу, всем файлам, группе файлов, запретить доступ к сайту и(или) определенных **ip**/подсетей; разрешить доступ с определенных **ip**/подсетей; установить пароль на директорию, файл, группу файлов; сделать редирект (перенаправление) на другой **URL** и еще многое другое.
IP-адрес	Уникальный, никогда не повторяющийся адрес компьютера в сети интернет. Обычно разбивается на четыре секции и имеет вид **132.234.765.654**
Mailing List (Mail List)	Список рассылки. Чаще используется для спама, предназначен для оповещения большого числа пользователей одним письмом
MySQL	Многопоточный сервер баз данных. **MySQL** имеет большую скорость, устойчивость и легкость в использовании **Perl** - универсальный язык программирования.
PHP	Язык для создания динамических страниц и написания скриптов. Одно из самых популярных средств написания сайта.
PHPMyAdmin	**WEB**-интерфейс для администрирования и работы с базами данных **MySQL,** предоставляет собой набор возможностей по созданию, удалению, изменению, экспору данных и т.д.
PostgreSQL	**SQL**-сервер - транзакции. Обладающий широкими возможностями храния процедур, триггеров и пр.
POP3, SMTP, IMAP	Протоколы для работы с электронной почтой. **Python** - универсальный интерпретируемый язык программирования. Так же применяется для написания **cgi**-скриптов. **TCP/IP** -основной протокол **Internet.**
Python	Универсальный интерпретируемый язык программирования. Так же применяется для написания **cgi**-скриптов.
TCP/IP	Основной протокол **Internet.**
SSI	Технология составления **html**-документов из нескольких файлов и связи их в единое целое. Позволяет включить в **Web**-страницу информацию на сервере, недоступную простыми средствами **HTML.** Например, если Вам нужно поменять одну и ту-же информацию на многих страницах сайта, достаточно это сделать на одной из страниц и при наличии поддержки директивы **SSI** и записи в файле **.htaccess** соответсвующие команды, содержимое измениться на всех указанных страницах
SSL (Secure Socket Layer)	Протокол шифрования конфеденциальных данных пользователя гарантирующий посетителям Вашего сайта, что их частная информация находится в безопасности с **SSL** свидетельством.
SSH	Протокол шифрования безопасного соединения и режим доступа на сервер.
SQL	Стандартизированный язык сохранения баз данных.
WAP	протокол для создания **WAP**-страниц, для просмотра с сотовых телефонов и прочих мобильных устройств, поддерживающих **WAP.** Позволяет с мобильных телефонов подключаться к сети **Internet.**
WEB-интерфейс	Для работы с почтой с любого подключенного к Интернет компьютера, на котором установлен **web**-броузер.

WHOIS	Программа, обращается с запросами к базам данных для получения информации, о пользователях и ресурсах интернета(домены, сети, хосты) и информации о пользователях сети(адрес, телефон, **e-mail**).
Бан сайта	от англ. **to ban** – запретить. Жаргонное выражение, означающее запрет сайта для индексирования и ранжирования модератором поисковой системы. Обычно применяется к сайту, применяющему методы поискового спама?. Следует отличать бан сайта от различного вида пессимизации сайта.
Дорвей	Входная страница **(Doorway)** - страница сайта, оптимизированная под одну или несколько поисковых фраз с целью попадания на высокие места в результатах поиска. Автоматически созданная входная страница содержит случайный текст, в котором периодически встречается нужная поисковая фраза, и потому не приносит посетителю никакой пользы.
Семантическим ядром	Рейтинг видимости рассчитывается для определенного конечного множества запросов, по которым оценивается продвижение сайта в поисковых системах. Это множество называется семантическим ядром.
Клоакинг (Cloaking)	от английского **to cloak** (маскировать) - Способ работы веб-сервера, когда пользователю показывается одно содержимое, а поисковому роботу - другое, благодаря которому страница и находится высоко в результатах поиска. Основывается клоакинг на отслеживании **IP**-адресов поисковых роботов и выдачи им заранее определенной информации.
Конверсия	Англ. **conversion ratio, CR** Отношение количества посетителей веб-сайта, совершивших целевое действие – клик, регистрацию, звонок, покупку и т.д. – к общему количеству привлеченных посетителей.
Пессимизация сайта	Эффект необычно низкого ранжирования сайта, возникший вследствие злоупотребления при продвижении сайта методами поискового спама. Подобный вид «наказания» применяется автоматически и, как правило, отсеивает наиболее массовые и доступные неопытным вебмастерам злоупотребления.
PPC	Это аббревиатура от **Pay-Per-Click**, по-русски это переводится как Оплата За Клик
Продвижение сайта	Комплекс мер, направленный на повышение целевой посещаемости сайта. В контексте **SEO** речь идет о повышении посещаемости сайта средствами поисковой оптимизации и контекстной рекламы.
Сниппет	От англ. **snippet** – фрагмент, отрывок. небольшие отрывки текста найденной поисковой машиной страницы сайта, использующиеся в качестве описания ссылки в результатах поиска. Как правило, подают контекст, в котором встретилось ключевое слово в тексте.
«CEO» SEO-Search engine optimization	Оптимизация сайтов для поисковых систем.
СЕРП-SERP	Англ. От **Search engine results pages.** Результаты Поиска.
Статические факторы	Факторы, учитываемые при ранжировании документа в результатах поиска без учета конкретного запроса. К примеру, такими факторами являются **PageRank** или ВИЦ.
ACPI	Расширенный интерфейс конфигурирования компьютера и управления питанием. Интерфейс **ACPI**, являющийся одним из элементов шины **SMBus**, позволяет переводить процессор в режим пониженного энергопотребления и экономить энергию в периоды бездействия.
AGP (Accelerated Graphics Port)	Ускоренный графический порт - интерфейс для подключения видеоадаптера к отдельной магистрали **AGP**, имеющей выход непосредственно на системную память.
BIOS	(базовая система ввода-вывода) - один из основных элементов персонального компьютера, программа, которую выполняет процессор, чтобы запустить компьютер после включения. Кроме того, **BIOS** управляет обменом данными между операционной системой компьютера и подключенными к нему периферийными устройствами.

Bluetooth	Международная инициатива компаний **Ericsson**, **IBM**, **Intel**, **Nokia** и **Toshiba**, направленная на установление стандарта беспроводного соединения между телефонами мобильной связи, ПК, ручными компьютерами и другими периферийными устройствами. Предусматривается использование малодистанционных (до 10 м) каналов в свободной полосе 2,45 ГГц, используемой научно-медицинскими приборами.
DDR SDRAM	Технология памяти **Double Data Rate (DDR) SDRAM** предусматривает передачу данных по обоим фронтам каждого тактового импульса, что позволяет удвоить пропускную способность памяти.
DVD (Digital Versatile Disk)	Цифровой универсальный диск - самый современный стандарт хранения информации на оптическом (лазерном) диске. Отличается от обычного **CD-ROM** увеличенной почти в 30 раз емкостью (до **17 GB**).
GPS (Global Positioning System)	**GPS** представляет собой спутниковую технологию позиционирования, которая позволяет при помощи **GPS**-приемника определять свои координаты в любой точке мира.
LAN (Local Area Network)	ЛВС, локальная вычислительная сеть. Связывает устройства (такие, как ПК, серверы и концентраторы), покрывая сравнительно небольшие площади (обычно не больше этажа или в крайнем случае здания). ЛВС характеризуются высокой скоростью передачи данных на короткие участки. Для построения ЛВС широко применяются технологии **Ethernet**, **FDDI** и **Token Ring**.
LCD-дисплей	Жидко-кристаллический (**Liquid Crystal**) дисплей (ЖК-дисплей). Для изготовления ЖК-дисплеев портативных компьютеров используют нематические кристаллы, молекулы которых, находясь между двумя стеклами с прозрачными электродами, в отсутствие электрического тока образуют спирали, скрученные (**twisted**) на 90 градусов.
Li-Ion	Аккумуляторы ионно-литиевые - существует два типа: с анодом из кокса и графита. Обладают существенно лучшими параметрами по энергетической емкости, чем **NiCd**- и **NiMH**-аккумуляторы. Ионно-литиевый аккумулятор работает в 1,5 раза дольше, весит на 25% меньше, чем никель-металл-гидридный.
PS/2 Port	Заимствован из архитектуры **IBM Micro Channel Architecture**, где данные передаются по 16- или 32-разрядной шине. К порту **PS/2** подключаются мыши и клавиатуры.
Wi-Fi	Общее название оборудования, соответствующего стандарту **802.11b** для беспроводных устройств, определенного организацией **Wi-Fi Alliance**.
Wireless USB Network Adapter	(беспроводной сетевой адаптер для шины **USB**) Устройство, соединяющее ПК с беспроводной сетью, используя порт **USB** компьютера вместо подключения к разъему **CardBus** или шине **PCI**.
Горячие клавиши (Hot Keys)	Комбинации клавиш, используемые для оперативного изменения параметров компьютера или свойств используемой программы.
Кэш	Блок высокоскоростной памяти, в которую копируются данные, извлеченные из оперативной памяти.
Proxy сервер	Буферный сервер, предназначенный для ускорения доступа, кэширования передаваемой информации и скрытия информации пользователя.
JavaScript (Java-скрипт, яваскрипт)	Язык обработки сценариев, позволяющий выполнять на компьютере пользователя определенные действия с **HTML**-страницами и объектами, размещенными на ней.
Баннер	от англ. **banner** – флаг) – подвижная (анимированная) или неподвижная (статичная) рекламная картинка, обычно прямоугольной формы. Является ссылкой, по которой можно перейти на страницу, где размещена информация о рекламируемом товаре.
Аутентификация	Проверка личности пользователя, как правило осуществляется с помощью пароля, **PIN**-кода или цифрового сертификата.
Браузер	(от англ. **browse** - листать) – программа для просмотра ресурсов и скачивания файлов.

Блог	(сокр. от англ. **weblog** – сетевой журнал) – Веб-страница, на которой записи расположены в порядке времени. Часто блогом называют Живой Журнал (ЖЖ) - личный дневник, выложенный в открытом доступе в Сети. Автор дневника регулярно пополняет его новыми записями, чтобы поддержать к нему интерес.
Вебмастер	Человек, который отвечает за внешний вид и работу сайта. Обычно именно к вебмастеру может обратиться пользователь, столкнувшийся на сайте с каким-то проблемами.
Виртуальный	(от англ. **virtual** - мнимый) – создающий видимость, ненастоящий. Обычно используется в словосочетании «виртуальная реальность». Впервые появилось в научной фантастике для обозначения искусственно созданного иллюзорного мира, ощущаемого как реальный. Теперь термином «виртуальная реальность» или «виртуал» иногда называют интернет, хотя это явное преувеличение.
Гипертекст	Документ, в тексте которого содержатся ссылки на другие документы. Ссылка для пользователя имеет вид подчёркнутого текста. Кликнув по ссылке, пользователь переходит на обозначаемый ею ресурс.
Игнор	(разг., от англ. **ignore** - игнорировать) – отказ посетителя чата или форума от общения с другим посетителем. Обычно «отправляют в игнор» грубиянов и просто назойливых собеседников. Функция «отправить в игнор» есть почти во всех чатах и форумах.
Интернет-магазин	Магазин, "витрина" которого расположена в Интернете. Прочитав описание продукта на сайте, посмотрев его фото и изучив цены, можно оформить заказ. Обычно товар доставляется курьером или по почте. Оплата производится наличными при получении, наложным платежом или переводом денег со счета. В интернет-магазинах можно купить практически все те же товары, что и в обычных - продукты питания, напитки, бытовую химию, книги, диски и т.д.
Интерфейс	(от англ. **interface** – стык, область контакта) – способ взаимодействия пользователя и компьютерной программы. Удобный в обращении интерфейс обычно называют «дружественным».
Модем	Устройство для преобразования полученных от компьютера сигналов в форму, годную для передачи по телефонной линии. При приеме входящего сигнала модем производит обратную операцию.
Модератор	Хозяин чата или форума, устанавливающий для пользователей правила поведения на его сайте и контролирующий их выполнение. Нарушителя правил (например, употребляющего ненормативную лексику) модератор может лишить права голоса или запретить ему доступ к сайту (на время или насовсем).
Мультимедиа	(от англ. **multi** - много и **media** - носитель, среда) - аудио и видео в Интернете. При скачивании мультимедиа следует помнить, что размер аудио и видео файлов обычно намного превышает размер файлов, содержащих только текст.
Навигация	Переход от одной веб-страницы на другую при помощи ссылок.
Он-лайн	(от англ. **on line** – на связи) - состояние, в котором компьютер соединён с сервером провайдера в интернет, то есть находится в Сети. Противоположность - офф-лайн (компьютер отключен от сети Интернет).
Офф-топик	(от англ. **off topic** – вне темы) - сообщение, не соответствующее тематике форума. Вызывает раздражение других пользователей и модератора.
Ошибка 403	Если пользователь, запросив веб-страницу, вместо нее получает сообщение об ошибке **403**, это означает, что доступ к странице запрещен. Это может случиться, если хозяин сайта решил закрыть от пользователей часть информации.
Ошибка 404	Если пользователь, запросив страницу, вместо нее получает сообщение об ошибке **404**, это означает, что запрошенному **URL** не соответствует никакая страница сайта. Это происходит потому, что ссылка неверна или ранее существовавшая страница была удалена.

Поисковая система	Инструмент для поиска информации в интернете. Пользователь пишет запрос (например, «ночные клубы Нижнего Новгорода») и получает список ссылок на ресурсы, где фигурируют заданные им слова. Поисковые машины различаются по области действия на локальные (ограничивающиеся национальным доменом или определенным языком) и глобальные. Первыми отображаются ссылки на документы, наиболее полно соответствующие запросу (релевантные).
Портал	Сайт, на котором собраны ссылки на другие сайты, обычно объединенные определенной тематикой, например, игровой портал. Обычно у портала много посетителей, он известен широкому кругу пользователей.
Провайдер	(от англ. **provide** - предоставлять) - компания, предоставляющая услуги доступа в интернет.
Ресурс	Информация (текст, музыка, видео, программное обеспечение и т.д.) в Интернет. Иногда используется как синоним слов сайт или веб-страница.
Сабж	Разг., от англ. **subject** - тема) - предмет, о котором идет речь в электронном письме, форуме и т.д.
Сервер	(от англ. **serve** – обслуживать) – слово употребляется в трех различных значениях.
Сисадмин	(разг., от англ. **system administrator** - системный администратор) - сотрудник, который отвечает за бесперебойную работу компьютеров и сетей, а также за информационную безопасность компании.
Служба знакомств	Сайт, помогающий людям найти новых знакомых. Обычно представляет собой базу данных, где можно оставить анкету с информацией о себе и сформулировать свои пожелания (по аналогии с рубрикой «Знакомства» в обычной газете), а также просмотреть информацию о других пользователях. Информация подается анонимно и может не соответствовать реальности, поэтому при поиске друзей через службу знакомств следует проявлять осмотрительность.
Смайл	(от англ. **smile** - улыбка) - знак, составленный из знаков препинания, букв и цифр, передающий эмоции пользователя во время общения в Интернете. Обычно это изображение «рожицы», положенной на бок. Например **:-)** означает радость или веселье, **:-(** - отрицательные эмоции, **8-0** – удивление и т.д.
Троянский конь	(миф., разг. "троян", "троянец") - вредоносная программа, скрытно проникающая на компьютер пользователя, очень часто под видом чего-либо безобидного - "крэка программы", "ускорителя интернет", "игры" и т.п., служащая для получения злоумышленником информации с компьютера пользователя или для получения доступа к компьютеру.
Учетная запись	описание пользователя, которое хранится на компьютере. Обычно включает в себя имя пользователя в системе, настоящее имя, пароль, права пользователя.
Файрвол	(от англ. **firewall** - противопожарная стена), межсетевой экран, брандмауэр - программа или компьютер, используемые для защиты компьютерных сетей или одного компьютера (персональный файрвол) от несанкционированного доступа (взлома). Основной принцип работы файрвола - запрет определенных типов трафика, что не позволяет обращаться к защищаемому компьютеру или сети из интернет.
Форум	место для общения на сайте. Как правило, форум имеет определенную тематику, например «Отзывы о нашем сайте», «Здоровье», «Автомобили», «Форум для мам», «Интернет-форум» и т.д. Пользователь оставляет свое сообщение, в котором предлагает другим участникам форума высказать свое мнение на определенную тему, например «Как почистить дубленку, не отдавая ее в химчистку?» и ждет их ответов и уточняющих вопросов. Если заявленная тема интересна, в дискуссию вовлекается большое число участников. Работу форума контролирует его модератор. В отличие от чатов, сообщения, отправленные в форум, могут храниться очень долго.

Хакер	(от англ. **hack** – рубить, кромсать) - изначально - человек интересующийся компьютерами, пытающийся вникнуть в суть работы компьютеров, сетей или программ. Термин пришел из Массачусетского технологического института (**MIT**). В настоящее время чаще используется как синоним термина "компьютерный преступник".
ЧаВО	часто задаваемые вопросы, см. **FAQ**.
Чат	(от англ. **to chat** - болтать) – место для общения в интернете, где пользователи обмениваются сообщениями в реальном времени. Все сообщения всех участников непрерывным потоком проходят перед глазами пользователя, из этого потока он выделяет те, что адресованы лично ему или всем участникам чата.
MP3	Формат аудиофайлов, широко распространенный в интернете. В интернете существует большое количество **mp3**-архивов (музыкальных коллекций), откуда можно скачать нужную композицию за плату или даром.
URL	(от англ. **Universal Resource Locator** – универсальный код расположения ресурса) – уникальный адрес веб-страницы на сервере. Очень часто ошибочно используется вместо термина **URI** (**Unified Resource Identificator**) - уникальный идентификатор ресурса в **Internet**, например **Web**-страницы **http://www.webtopit.com/**
ИМХО	Аббревиата **IMHO (in my humble opinion** - по моему скромному мнению). Аналог русского - "я думаю", "я полагаю", "мне кажется".
ФАГ	Транслитерация **FAQ (frequently asked questions** - часто задаваемые вопросы). Подразумеваются не только сами вопросы, но и ответы на них.
ЗЫ	**P.S.** = Постскриптум. Получается, если не переключиться на латинский шрифт при наборе **P.S.** и пропустить точки.
AFAIK/AFAIR	**As Far As I Know/Remember** - насколько я знаю/помню
FYI	**For You Info.** Перевод : "Шоб ты знал!"
RTFM	**Read This F$%king Manual** или "Если ничего не выходит - прочтите наконец инструкцию". Или как вариант **RTFF** - то же самое, только читать надо **FAQ**.
Флейм	Очень длинное обсуждение какого-либо вопроса, участники которого давно забыли первоначальный вопрос, перешли на личности и вспомнили старые обиды и противоречия.
STFU	(англ. «**Shut the FuckUp**») – «Закройте свой рот»
WTF	(англ. «**What the Fuck**») – «Чё за фигня?»
BTW	(англ. **By The Way** - кстати) "**BTW**, как там твоя программа?"
LMD	(англ. «**Lamers Must Die**») - Ламеры должны умереть
Suxx	Существует множество легенд о происхождении (этимологии) этого слова. Означает оно "плохо". Например: "Плохая погода" - "Погода **suxx**" или "**suxx**-ная погода". Произносить это слово можно и как "сакс" и "сукс", а некоторые люди говорят "суксь". (Надо отметить, что слово "сакс" некоторые люди могут понять как "саксофон"). Писать это слово можно и с одной буквой "**x**". Вообще, считается что с помощью слов "**Suxx**", "Рулез", "**MustDie**", "Бага" и "Фича" можно выразить любое, сколь угодное сложное чувство.
Рулёз, РУлез, РулЕз.	Тоесть хорошо, классно, супер, шикарно. Чуство радости о чём то. Например "рулёзная погода" или "рулёзное настроение" или "пиво - рулез".
E-mail, EML, емеля, мыло	Электронная почта.
ИК	Инфракрасный.
ИТ	Информационные технологии.
ОС	Операционная система.
ПО	Программное обеспечение.
Фича (от английского Feature)	Это некоторая особенность, функция чего-либо. Например, бывают мыши с колёсиком для прокрутки и без. Так вот колёсико - фича. Бывают мышки беспроводные. Это тоже фича. Это слово чаще всего используется для описания особенностей программ.

GIF	**(Graphics Interchange Format) -** В **GIF** (гифах) можно хранить анимационные картинки. Здесь используется алгоритм сжатия иной, чем в **JPEG**, и неприемлемый для фотографий. **GIF** картинки не могут содержать более **256** цветов. Но в них очень удобно хранить несложные элементы оформления сайтов и баннеры.
HTTP	**(HyperText Transfer Protocol) -** Это, как следует из названия, протокол передачи гипертекста. А если перевести на русский язык, так просто сайтов. Именно этим протоколом пользуются броузеры и серверы, на которых расположены сайты. В **URL**`е любого сайта (и всех других ресурсов Сети тоже) первым делом указывается протокол (например: **http://www.webtopit.com)**
IRC	**(Internet Relay Chat) –** Чат работающий по принципу: Сервер – Клиент. Есть программка у вас, и с ней вы подключаетесь к разным серверам, в разные комнаты, и общяетесь.
Ping	Эта программа в чём-то схожа с игрой в пинг-понг. Она посылает на какой-то компьютер в интернете немного данных, а этот компьютер должен послать этот "мячик" назад. Таким образом, можно проверять наличие связи с удалённым компьютером, а также скорость передачи данных на удалённый компьютер. Это бывает очень важно в **on-line** играх.
Telnet	Эта программа позволяет удалённо работать на другом компьютере. В основном, используется всякими сисадминами для удалённого администрирования. Простым смертным она вряд ли понадобится.
Web-дизайн, Веб-дизайн.	Цветовая гамма, графика, украшения и навороты на сайте, являються дизайном. Так же как и дизайн квартиры, только речь о сайтах.
Windows, Винда, Форточки	**MS Windows -** это операционная система - самая главная программа на компьютере **.Windows -** с английского переводится «окна», отсюда и название "форточки".
Апплет	Небольшая программа для интернета запускаемая броузером и работающая на компьютере пользователя (клиентской). Апплеты написанные на языке **Java** будут одинаково исполнятся на любом компьютере.
Баг (Англ. Bug - жучок)	Баг - глюк, ошибка. Отсюда дебагер **(debuger)** - программа для поиска ошибок в программах, т.е. жучков, забравшихся в программу.
Выделенка	Выделенная линия. Такая обычная телефонная линия проводится телефонной компанией в квартиру, но использует только для интернета. Поэтому качество связи лучше, скорость может быть больше во много раз чем по телефонной линии, и пользоваться ей можно круглосуточно, не занимая обычного голосового телефона.
Звонилка	Программа для дозвона к провайдеру. Умеет перезванивать при обрыве связи, перебирать несколько телефонных номеров, запускать аську при соединении, считать количество потраченных денег.
Скрипт	**(Script -** сценарий) **-** Скрипт - это небольшая программа. На веб-страничках скрипты используются для создания каких-нибудь специальных эфектов. Например, изменение картинки при наведении на неё мыши.

Благодарности.

Спасибо сайтам:

Prsiterun, Sandy, Skyfamily – За помощь в составление словаря терминов и сленга. К сожалению, в данной сборке собраны не все слова. Наш интернет настолько огромная сеть, что для того, чтобы собрать все сленговые слова, и термины, понадобилась бы не одна книга.

Сайт **Wikipedia**, и сайт **Yandex–** за то, что помогали в определении терминов и описание тех или иных слов.

Спасибо ру-нету, за собрание статей и рассказов. Хочу поблагодарить Билла Гейтса **(Bill Gates)**, за то, что предоставил программу **Office Word 2007**, которая помогла оформить книгу, и проверить книгу на орфографию. А так же разработчиков из фирмы **FinePrint SoftWare**, за программу **PDFfactory**.

Контакты

Данную книгу собрал и подготовил Андрей Игоревич.

Ник в сети: -=[MaPuK]=-

ICQ: 562778

E-mail: **cyxapuka@gmail.com**

WebSite: **www.webtopit.com**

Donate

Если вы хотите выразить свою благодарность, вы можете отправить немного денег на мой кошелёк в системе **WebMoney**.

R766535086696 – Рубли.

Z170657151372 – Доллары **USD**.

Автор писал книгу 83 дня.